Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.046757

ARTICLE

A Hybrid Cybersecurity Algorithm for Digital Image Transmission over Advanced Communication Channel Models

Naglaa F. Soliman[1], Fatma E. Fadl-Allah[2], Walid El-Shafai[3,4,*], Mahmoud I. Aly[2], Maali Alabdulhafith[1] and Fathi E. Abd El-Samie[1]

[1]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia

[2]Department of Electronics and Communications, Faculty of Engineering, Zagazig University, Zagazig, 44519, Egypt

[3]Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh, 11586, Saudi Arabia

[4]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt

*Corresponding Author: Walid El-Shafai. Email: walid.elshafai@el-eng.menofia.edu.eg

Received: 13 October 2023 Accepted: 29 December 2023 Published: 25 April 2024

ABSTRACT

The efficient transmission of images, which plays a large role in wireless communication systems, poses a significant challenge in the growth of multimedia technology. High-quality images require well-tuned communication standards. The Single Carrier Frequency Division Multiple Access (SC-FDMA) is adopted for broadband wireless communications, because of its low sensitivity to carrier frequency offsets and low Peak-to-Average Power Ratio (PAPR). Data transmission through open-channel networks requires much concentration on security, reliability, and integrity. The data need a space away from unauthorized access, modification, or deletion. These requirements are to be fulfilled by digital image watermarking and encryption. This paper is mainly concerned with secure image communication over the wireless SC-FDMA system as an adopted communication standard. It introduces a robust image communication framework over SC-FDMA that comprises digital image watermarking and encryption to improve image security, while maintaining a high-quality reconstruction of images at the receiver side. The proposed framework allows image watermarking based on the Discrete Cosine Transform (DCT) merged with the Singular Value Decomposition (SVD) in the so-called DCT-SVD watermarking. In addition, image encryption is implemented based on chaos and DNA encoding. The encrypted watermarked images are then transmitted through the wireless SC-FDMA system. The linear Minimum Mean Square Error (MMSE) equalizer is investigated in this paper to mitigate the effect of channel fading and noise on the transmitted images. Two subcarrier mapping schemes, namely localized and interleaved schemes, are compared in this paper. The study depends on different channel models, namely Pedestrian A and Vehicular A, with a modulation technique named Quadrature Amplitude Modulation (QAM). Extensive simulation experiments are conducted and introduced in this paper for efficient transmission of encrypted watermarked images. In addition, different variants of SC-FDMA based on the Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Fast Fourier Transform (FFT) are considered and compared for the image communication task. The simulation results and comparison demonstrate clearly that DWT-SC-FDMA is better suited to the transmission of the digital images in the case of Pedestrian A channels, while the DCT-SC-FDMA is better suited to the transmission of the digital images in the case of Vehicular A channels.

KEYWORDS
Cybersecurity applications; image transmission; channel models; modulation techniques; watermarking and encryption

1 Introduction

Wireless image transmission is widely employed in many different applications in our lives such as remote sensing via satellite, nuclear medicine, telemedicine, teleconferencing, broadcast television, and accessing Internet services on mobile phones. Therefore, the increasing demands for wireless image transmission have recently attracted the attention of a lot of researchers. Hence, much research work and studies have been done to develop numerous techniques for image transmission over wireless noisy channels. These techniques are improved from one generation to another [1]. One of the most recent techniques that were developed is the Single Carrier Frequency Division Multiple Access (SC-FDMA) [2,3].

Since the Internet has grown in popularity, and individuals can share whatever they want to share like images, videos, documents, etc., there has been a need to preserve publishing copyright. Additionally, there has been a high demand for information security. For these and other reasons, digital image watermarking has gained a large popularity in recent years as a good solution in such cases. Much researchers have worked in this field to create new techniques, and to improve existing procedures as proper solutions for the above-mentioned problems [4]. To increase the security to some extent, sometimes an encryption procedure is also used along with a watermarking algorithm. The combination of digital watermarking and encryption techniques can be used to achieve a higher degree of security.

In the contemporary era, the surge in multimedia applications and smart devices has exponentially amplified the demand for efficient transmission of digital images. As image transmission constitutes a substantial portion of wireless communication systems, it has become imperative to ensure that communication standards are optimized for high-quality image transmission. However, while the technical specifications are being advanced, it has become increasingly evident that security cannot be sidelined. Recent statistics indicate that nearly 95% of multimedia data breaches were attributed to the insecure transmission of digital images [5]. Furthermore, real-world scenarios, such as the dissemination of critical surveillance imagery, telemedicine where patients' diagnostic imagery is transmitted, or even satellite image communications, emphasize the paramount need for secure transmission methodologies. Any compromise in these domains can lead to devastating consequences, ranging from privacy invasion to national security threats. In the broader landscape of wireless communication, SC-FDMA has garnered attention, particularly as an uplink standard in mobile communication systems. This underscores the pertinence of studying secure image communication tailored for this system. While open-channel networks facilitate a multitude of data transmission, they are also prone to vulnerabilities. Unauthorized access, inadvertent modifications, or even unintentional deletions can jeopardize the integrity and reliability of the transmitted data. Such challenges are further amplified in the realm of image transmission, making it a critical area of research. Considering the above-mentioned issues, this paper delves into the intricacies of secure image communication over the wireless SC-FDMA system. We have anchored our research on a robust image communication framework optimized for SC-FDMA, aiming to strike a balance between enhanced image security

and impeccable quality at the receiving end. Thus, through this research, we aim to bridge the existing gaps and offer a fortified, efficient, and reliable solution for digital image transmission in the current digital age, where both quality and security are of utmost importance.

With the burgeoning growth in multimedia technology and the paramount importance of digital image transmission in wireless communication systems, there exists a persistent challenge: How can we ensure both efficient transmission and robust security for images in an SC-FDMA system, which remains a pivotal standard in mobile communications?

This research, therefore, aims to:

- ***Introduce a Robust Framework:*** We propose a novel framework for secure image communication over the SC-FDMA system. This framework should not only safeguard images from unauthorized access, modification, or deletion but also guarantee their high-quality reconstruction at the receiver end.
- ***Merge Watermarking & Encryption:*** We implement a unique hybrid approach of digital image watermarking, based on the Discrete Cosine Transform (DCT) merged with the Singular Value Decomposition (SVD) (DCT-SVD watermarking), and encryption based on chaos and Deoxyribonucleic Acid (DNA) encoding. The amalgamation of these techniques is hypothesized to provide an enhanced level of security for image data, a feat that individual methods might fall short of.
- ***Evaluate Performance in Diverse Conditions:*** We study the efficiency and security of our proposed method under different channel conditions, modulation techniques, and SC-FDMA variants. The goal is to ascertain the adaptability and reliability of our method in real-world scenarios, which is vital for practical applications.
- ***Optimize Performance for Channel Types:*** We determine the most suitable SC-FDMA variant for specific channel models, such as Pedestrian A and Vehicular A channels, to ensure optimal performance based on the environment.

In essence, our primary objective is to address the dual challenge of ensuring robust cybersecurity while maintaining the integrity and quality of digital images during transmission over advanced communication channel models, specifically the SC-FDMA system. We believe that a successful implementation of our proposed methods will significantly advance the field of secure image communication and set new benchmarks for future endeavors.

Therefore, this paper is directed to the study of image communication over the wireless SC-FDMA system. Different tools are investigated for this task to send images with high quality and high security over the SC-FDMA system. The digital images are processed through a two-level security mechanism before the communication process. These two levels depend on the DCT-SVD hybrid image watermarking algorithm as the first stage followed by image encryption as a second stage. Chaos and DNA encoding rules are considered for the task of image encryption. The resulting encrypted watermarked image is then transmitted over the SC-FDMA system. The communication tool considered to mitigate the channel effects is equalization. Linear Minimum Mean Squared Error (MMSE) equalizer is considered in this work.

The linear MMSE equalizer is an essential tool in modern communication systems, particularly in mitigating the adverse effects of channel fading and noise. Unlike other linear equalizers, the MMSE equalizer aims to minimize the mean square error between the estimated and actual transmitted signals. This approach offers an advantage, especially in environments with considerable noise and interference. To understand its operation, let us briefly discuss the underlying principle. In a

communication channel, the transmitted signal gets distorted due to various factors, including fading and noise. The equalizer role is to reverse or compensate for this distortion to retrieve the original signal at the receiver side. The linear MMSE equalizer does so by adapting its filter coefficients in a way that the Mean Square Error (MSE) between the original and estimated signals is minimized. In the context of our study, where image transmission is of paramount importance, the MMSE equalizer plays a pivotal role. Images are inherently high data-rate signals, making them more susceptible to errors due to channel impairments. The MMSE equalizer, with its adaptive nature, ensures that these images are received with minimum distortion, maintaining their integrity and quality. This is especially crucial in wireless communication scenarios, where channel conditions may vary rapidly. For the SC-FDMA system, which inherently has a low Peak-to-Average Power Ratio (PAPR) and low sensitivity to carrier frequency offsets, the role of the MMSE equalizer becomes even more relevant. It not only combats the effects of channel fading and noise but also synergizes with the SC-FDMA system properties, ensuring secure and efficient transmission of images. In conclusion, the linear MMSE equalizer is not just a tool but a vital component in our proposed framework, ensuring that the transmitted images are received with the highest possible fidelity even in challenging channel conditions.

In our pursuit to address the challenges of digital image transmission over advanced communication channels, this research contributes in several novel ways. The main contributions of the paper can be summarized in the following points:

- ***Hybrid Security Mechanism:*** While individual methodologies for watermarking and encryption have been explored in past research, our work introduces a hybrid model that synergistically integrates the DCT with the SVD (DCT-SVD) watermarking and chaos-based DNA encoding for image encryption. This layered approach ensures enhanced robustness against potential security threats.
- ***Optimization for SC-FDMA:*** Tailoring a cybersecurity algorithm specifically for the SC-FDMA system, which is a cornerstone in modern broadband wireless communications, is a distinguishing aspect of this research. By tapping into the inherent advantages of SC-FDMA, we ensure that our security solutions are not only potent but also in sync with prevalent communication standards.
- ***In-Depth Channel Model Analysis:*** A unique feature of our study is the comprehensive assessment performed on different types of channel models, specifically 'Pedestrian A' and 'Vehicular A'. This granular analysis offers insights into how our algorithm performs under varying transmission conditions, ensuring its wide applicability.
- ***Comparative Study of SC-FDMA Variants:*** An added dimension of novelty is our comparative study on the different variants of SC-FDMA based on Fast Fourier Transform (FFT), DCT, and Discrete Wavelet Transform (DWT). To the best of our knowledge, such an exhaustive comparative analysis, specifically in the context of digital image transmission, has not been undertaken before. Our results highlight the most efficient variant for specific channel conditions, providing practical insights for real-world deployments.
- The encrypted digital watermarked image is transmitted over a wireless SC-FDMA system. Different arrangements and scenarios are considered for the communication segment of the proposed framework to set up the communication architecture. These scenarios include:
    - ◯ Two subcarrier mapping schemes, namely localized and interleaved subcarrier mapping,
    - ◯ MMSE equalizer to mitigate the channel effects at the receiver part,
    - ◯ Three versions of the SC-FDMA system, namely DWT-SC-FDMA, DCT-SC-FDMA, and FFT-SC-FDMA, to select the most appropriate modulation scenario for image communication, and

- ◯ Two different wireless channel models, namely Pedestrian A and Vehicular A, to investigate the effect of channel degradations on images in each scenario.
- The decrypted watermarks are extracted after the communication scenario and the effects of all processes adopted in the suggested framework are studied.

In summary, our work bridges the gap between robust cybersecurity measures and efficient digital image transmission in wireless communication systems, making a significant stride in the domain of multimedia technology.

2 Related Works

This paper presents a powerful security algorithm for image communication through merging digital image watermarking with image encryption techniques. The goal of this merging technique is to enhance and strengthen image security through its transmission over the wireless SC-FDMA system [5]. In the literature, several methods have been proposed to develop image transmission over wireless communication systems. Some of these methods are reviewed in this section.

Bahaddad et al. proposed a modified Orthogonal Frequency-Division Multiplexing (OFDM) scheme for the transmission of images [6]. This proposal is based on modifying the OFDM structure by using unequal power allocation for the successive OFDM symbols. With unequal power allocation, an unequal cyclic time guard is also used. A comparison is carried out between this method and the conventional OFDM. Results demonstrate that the performance is enhanced with lower average powers and lower average cyclic extension periods when using this method. With and without Forward Error Correction (FEC), the performance of the OFDM scheme was examined. Simulation results proved that the utilization of FEC enhances the process of image communication.

Bhowmik and Acharyya studied watermarked image transmission in an OFDM system over the wireless Additive White Gaussian Noise (AWGN) channel using a 256-Phase-Shift Keying (PSK) modulation scheme. The transmission performance analysis has been carried out [7]. The Peak Signal-to-Noise Ratio (PSNR) has been used to assess the visual quality of watermarked images. Cox's algorithm has been used to extract the watermark from the received image. The statistical correlation parameter and the Bit Error Rate (BER) have been used as assessment tools for the recovered watermarks. Two distinct modulation schemes, namely 16-PSK and 16-Quadrature Amplitude Modulation (QAM), have been considered in this study for watermarked image communication. Simulation experiments at different Signal-to-Noise Ratio (SNR) values proved that 16-QAM is superior to 16-PSK for watermarked image communication to maintain the ability to recover the watermarks. The simulation results for the 16-QAM modulation scheme are further improved upon applying the Hamming (7, 4) for error correction to preserve the high quality of reconstructed images.

Faragallah et al. presented a robust procedure for medical image transmission with hidden patient information as a watermark [8]. The patient information is encoded as a watermark into the Least-Significant Bits (LSBs) of the medical image pixels in this procedure. This technique is some sort of spatial-domain digital watermarking. The watermark is encrypted to prevent unauthorized access to data. The encrypted watermark is coded by concatenation of Reed Solomon (RS) codes and Low-Density Parity Check (LDPC) codes to enhance the embedded information robustness. Even in the absence of noise, the accuracy of watermark extraction is dependent on the region of the medical image into which the watermark is embedded. As a result, the quality of the extracted watermark is assessed for three different regions of the image without noise. A wireless channel with burst errors has been considered in this study. Turbo coding has also been considered as a way to correct transmission errors

over the channels with impulsive noise. Simulation results proved the importance of Turbo coding for extracting highly-accurate watermarks.

Eichelberg et al. presented a study for secure color image communication over the SC-FDMA wireless communication system [9]. Chaos-based image encryption has been considered for this task. In addition, different decomposition equalization schemes have been considered and compared for the image communication task. Different modulation schemes have also been considered and compared for the task of encrypted image communication. Simulation results proved that a framework comprising chaos-encrypted images, QAM and convolutional coding with rate $1/2$ at the transmitter with ZF equalizer at the receiver is successful for image communication over Rayleigh multipath fading channels.

Eichelberg et al. proposed a Multi-Input Multi-Output Space Frequency Block Coding Orthogonal Frequency Division Multiplexing (MIMO-SFBC-OFDM) scheme for the transmission of medical images over frequency selective fading channels [10]. Its performance has been analyzed in comparison with that of the Single-Input Single-Output Orthogonal Frequency Division Multiplexing (SISO-OFDM) using Vertical-Bell Laboratories Layered Space-Time (V-BLAST) detection scheme at the receiver. The presented structure in this paper has been utilized for transmitting watermarked medical images with patient information as watermarks. Simulation results proved the superiority of the MIMO-SFBC-OFDM to the SISO-OFDM scheme in guaranteeing a secure and high-fidelity medical image communication process.

Hassan et al. proposed an efficient approach for the transmission of encrypted images with a Fast Fourier Transform (FFT) version of the OFDM system [11]. El-Shafai et al. presented a secured transmission scheme for watermarked images over the Long-Term Evolution (LTE) downlink physical layer [12]. The watermark images are first scrambled for better security. Then, they are embedded into the transform coefficients of the host image using a hybrid transform-domain technique. The watermarked image is transmitted over the OFDM downlink physical layer. Medical images have been transmitted over this scheme for remote automated diagnosis purposes. Hence, a classification task is performed on the received images. A Support Vector Machine (SVM) is used for the classification of the Non-Region of Interest (NRoI) and the Region of Interest (RoI) in the medical images. The results obtained with this framework have shown a 10^{-6} Bit Error Rate (BER) level for images transmitted at about 10 dB SNR. This is translated to high PSNR values of received images, and hence high quality of received image segmentation and classification.

Hassan et al. proposed an image transmission scheme with two levels of encryption to send images over OFDM channels. In this scheme, both bit-level scrambling and symbol scrambling are considered and combined [13]. Hassan et al. proposed an encryption scheme for image communication over OFDM [14]. Rubik's cube encryption technique has been adopted in this study to achieve better security and also to have better-quality received images. Two OFDM implementations based on FFT and DCT have been considered in the modulation process in this study. Different variants of modulation schemes have also been considered and compared in this work. It was observed from the numerical and visual inspection results that the Rubik's cube encryption algorithm is successful for image communication over DCT-OFDM. The DCT implementation of OFDM allows better energy compaction of transmitted signals in addition to less effect of frequency and phase offsets.

Faheem et al. presented an efficient transmission scheme for encrypted images through a MIMO–OFDM system over an AWGN channel [15]. Different encryption schemes have been considered and compared. Different encryption algorithms have been combined to improve the security of image communication. Jayakokela et al. proposed a methodology for embedding secret messages in

binary images. This methodology depends on LSB image steganography [16]. The stego-image is then transmitted over the SC-FDMA system. The embedded binary message is further extracted from the received stego-image at the receiver. Both PSNR and MSE have been considered to assess the quality of the stego image. To enhance the security of embedding, a double embedding process is adopted. Hence, secrecy is maintained during the communication process. A comparison between the SC-FDMA and the OFDMA for stego-image communication has proved that the SC-FDMA is preferred from the quality perspective.

As the quantum computing frontier rapidly advances, the traditional cryptographic algorithms, notably ECC and RSA, are exposed to vulnerabilities. Recognizing this, the arena of Post-Quantum Cryptography (PQC) has emerged, offering algorithms that anticipate and aim to counteract quantum computation threats. This evolution is vital for our research, as digital image transmission necessitates utmost security, especially in the quantum era. Integrating PQC into our proposed digital image watermarking and encryption methodologies ensures robustness against potential quantum attacks [17]. The work of [17] presented innovative approaches to ensuring security, emphasizing the significance of proactive measures in the wake of quantum computing advancements.

Side-channel attacks exploit physical information leaked during the execution of cryptographic operations. These can be power consumption patterns, electromagnetic radiations, and even execution times. Given our context of image transmission, it is imperative to consider these attacks, especially when such transmissions are performed on wireless devices susceptible to physical leakages. Lightweight cryptography offers a balanced approach, ensuring security while optimizing for efficiency—a crucial requirement for devices with resource constraints. We aim to delve into the nuances of lightweight cryptographic techniques and their applicability in the domain of digital image transmission over wireless networks. Given the resource limitations of many wireless devices, lightweight cryptography provides a promising direction for secure image transmission, while ensuring minimal overheads. The advent of quantum computers mandates the need for quantum-resistant cryptographic solutions. Within this subsection, we intend to expound on how PQC methods can be harmonized with our security framework, ensuring robustness against evolving quantum threats, especially when considering the transmission of sensitive images over advanced communication channels [17,18].

In modern wireless communication systems, there is a growing emphasis on conserving energy and ensuring low-power consumption, especially in mobile and edge devices. Lightweight Cryptography (LWC) becomes essential in such contexts as it offers cryptographic solutions that are optimized for power, energy, and area efficiency, without compromising security. The Camellia block cipher, as mentioned in [19], presents an excellent case for LWC. The paper delves into reliable architectures designed for the Camellia cipher, showcasing its adaptability for different variants of substitution boxes. Such design considerations are vital in ensuring that the cryptographic operations are not just secure but also energy-efficient, aligning with the objectives of LWC. As our proposed framework is focussed on the secure transmission of digital images, leveraging principles from LWC, like those exhibited by the Camellia block cipher, can greatly enhance the energy efficiency of our solution. Future implementations of our framework will indeed benefit from integrating these principles, ensuring a balance between robust, security and power conservation.

3 Preliminaries

3.1 SVD-Based Image Watermarking

In numerous applications, including watermarking, the SVD is extensively employed. Many methodologies for watermarking utilizing SVD have been introduced. These techniques involve embedding watermarks through alterations to the singular values **S** or the orthogonal vectors **U** and **V** in digital watermarking. The use of SVD in watermarking offers multiple benefits. A notable attribute of SVD is the robust stability of its singular value **S**. This characteristic ensures that the visual integrity of an image remains largely unaffected, even in the face of significant modifications due to attacks [17,18].

$$\mathbf{S} + \alpha \mathbf{W} = \mathbf{U}_{\mathbf{WHost}}\, \mathbf{S}_{\mathbf{WHost}}\, \mathbf{V}^{\mathbf{T}}_{\mathbf{WHost}} \tag{1}$$

where **S** represents the singular values of the host image, α denotes the scale factor used to control the strength of the watermark to be inserted and **W** is the watermark. The embedding method expressed by Eq. (1) is shown in Fig. 1. Finally the watermarked image $\mathbf{A}_w$ is obtained from the modified singular values $\mathbf{S}_{\mathrm{WHost}}$ and the vectors **U** and $\mathbf{V}^{\mathbf{T}}$ of the host image according to Eq. (2) [17–19].

$$\mathbf{A}_w = \mathbf{U}\mathbf{S}_{\mathbf{WHost}}\mathbf{V}^{\mathbf{T}} \tag{2}$$

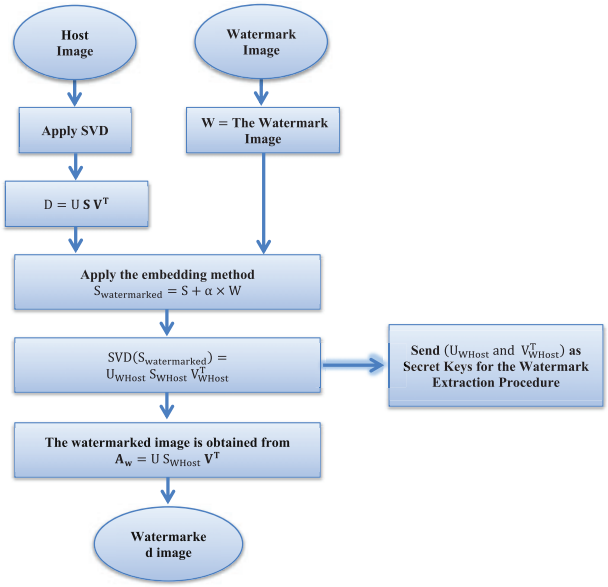


Figure 1: SVD-based image watermarking

3.2 DNA Sequence and Encoding

DNA is a molecule that contains the genetic information used in the growth, development, functioning, and reproduction of any living organism or virus [20]. In biology, a DNA sequence consists of four nucleotides, adenine (A), thymine (T), cytosine (C), and guanine (G). According to the complementary pairing rules of DNA, A is paired with T, and C is paired with G as shown in the double helix structure of the DNA in Fig. 2 [21]. In binary encoding, 0 and 1 are complementary. So, 00 and 11 are complementary, similar to 01 and 10. By using four bases A, C, G and T to encode 00,

01, 10 and 11, eight rules satisfy the complementary relations among the bases [20]. DNA coding rules are shown in Table 1 [22].

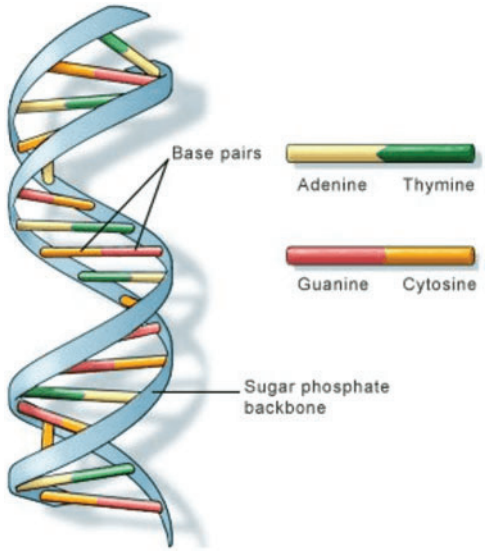


Figure 2: Double helix structure of the DNA

Table 1: Encoding and decoding rules

RULE	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

The XOR rule used by this algorithm for DNA sequences is similar to the traditional XOR rule. Therefore, the DNA XOR rule is shown in Table 2.

Table 2: DNA XOR operation

XOR	A	C	T	G
A	A	C	T	G
T	T	G	A	C
C	C	A	G	T
G	G	T	C	A

3.3 PWLCM and Logistic Map

The Piecewise Linear Chaotic Map (PWLCM) and logistic map are used to generate all parameters the algorithm requires. The PWLCM is described in Eq. (3), while the logistic map is defined by

Eq. (4) [22–24].

$$x_{n+1} = f_p(x_n) = \begin{cases} \dfrac{x_n}{p}, & 0 < x_n < p \\ \dfrac{x_n - p}{0.5 - p}, & p \le x_n < 0.5 \\ f_p(1 - x_n), & 0.5 \le x_n < 1 \end{cases} \tag{3}$$

$$x_{n+1} = \mu x_n (1 - x_n) \tag{4}$$

where $x_n \in (0, 1)$ and $p \in (0, 0.5)$. In experiments, we use $p = 0.25678900$ [25,26].

3.4 MD5 Hash Function

The Message-Digest (MD5) hash function is commonly used in encryption. It generates a 128-bit hash value typically presented as a 32-digit hexadecimal number, literally. The initial values are given by Eq. (5) [27–29].

$$x_0 = mod\,(d1 \oplus d2 \oplus d3 \oplus d4, 256)\,/255 \tag{5}$$

where x_0 is the initial value of the chaos map. d_1, d_2, d_3, and d_4 are extracted from the MD5 hash value of the plain image. We only need to transform d_1, d_2, d_3 and d_4 from binary to decimal, before using Eq. (5).

4 The Proposed Hybrid DCT-SVD Image Watermarking Algorithm

The continuous and rapid growth of multimedia technology has accentuated the criticality of efficient image transmission, especially in the realm of wireless communication systems. Achieving high-quality images in transmission, while essential, is only part of the puzzle; ensuring that security against an array of cyber threats is equally imperative. As a dominant force in broadband wireless communications, the Single Carrier Frequency Division Multiple Access (SC-FDMA) boasts features such as a low PAPR and diminished sensitivity to carrier frequency offsets. This makes it a focal point of our investigation, particularly as it remains a pivotal uplink standard in mobile communication systems.

Amid the myriad of challenges encompassing data transmission in open-channel networks, some stand out: ensuring data security, upholding its integrity, and guaranteeing its reliability. When we narrow this down to the domain of image transmission, the intricate nature of images demands robust measures to thwart unauthorized access, modification, or erasure. It is this very serious challenge that this paper addresses.

- **Roadmap of Our Research:**
  - ***Robust Framework for Image Security:*** At the heart of our study is the introduction of an innovative framework for secure image communication over the SC-FDMA system. This is not just about bolstering security but also ensuring that the images, once received, retain their quality.
  - ***Hybrid Approach with DCT-SVD Watermarking and Encryption:*** We employ a dual-pronged approach by merging digital image watermarking, leveraging the DCT combined with the SVD, with an encryption method rooted in chaos theory and DNA encoding principles.

- ***Evaluating MMSE Equalization:*** A pivotal component of our research will delve into the linear MMSE equalizer. Our goal is to ascertain and counteract the detrimental effects of channel fading and noise on images during their transmission phase.
- ***Comparative Analysis of SC-FDMA Variants:*** Given the diverse nature of communication channels, we will juxtapose different SC-FDMA variants: FFT, DCT, and DWT to deduce their efficacy in specific channel scenarios.
- ***Subcarrier Mapping Schemes and Channel Models:*** Our research will also encompass a comparative study of subcarrier mapping schemes, specifically localized and interleaved schemes. Furthermore, we will extend our investigation to different channel models, including Pedestrian A and Vehicular A, to ensure that our findings are applicable in real-world scenarios.

As we navigate through the intricate labyrinths of image transmission in the subsequent sections, we hope to provide readers with comprehensive insights, backed by extensive simulation experiments, into the most effective methods for secure and efficient image communication over advanced channel models.

The proposed algorithm has several significant contributions to the field of secure image communication over the SC-FDMA system:

- ***Hybrid Watermarking Technique:*** By merging DCT with SVD (DCT-SVD), we introduce a novel watermarking scheme. This approach not only enhances the robustness against various attacks but also retains a higher image quality, a balance rarely achieved by existing methods.
- ***Innovative Image Encryption:*** The paper presents a unique combination of chaos and DNA encoding techniques for image encryption. To our knowledge, this is the first work that synergistically integrates these two methods, resulting in enhanced security levels, especially for high-resolution images that are common in today's multimedia applications.
- ***Linear MMSE Equalizer Exploration:*** While the MMSE equalizer is known, its application in the context of SC-FDMA for secure image transmission, particularly with the challenges posed by watermarking and encryption, is a fresh area of exploration. Our findings provide valuable insights into mitigating channel fading and noise, crucial for real-world deployments.
- ***Comprehensive Analysis with SC-FDMA Variants:*** Our study is among the few that rigorously compare FFT, DCT, and DWT variants of SC-FDMA for the specific task of image communication. Our results present clear guidelines for practitioners on the choice of SC-FDMA variants based on channel conditions.
- ***Simulation-Driven Insights:*** Through extensive simulations, our research offers empirical evidence on the performance of different techniques across different channel models. These findings fill a gap in the literature, offering clear, actionable insights for researchers and industry professionals alike.

By addressing these areas, our research not only introduces novel methodologies but also serves as a comprehensive guide for secure image communication over the SC-FDMA system, paving the way for future investigations and practical implementations in this domain.

The DCT has found extensive applications in image processing due to its capability to transform an image into its constituent frequency components. SVD, on the other hand, is a mathematical operation that can decompose matrices in a way that makes them easier to analyze. When combined, DCT-SVD watermarking embeds watermark information into the significant frequency components of an image, ensuring that the watermark is robust against various attacks, while remaining imperceptible to the human eye. For a detailed understanding, readers are directed to [24]. A watermarking scheme

using DCT and SVD is introduced where the host image is transformed into Y,C_b,C_r planes using the popular RGB —YC_bC_r linear color transformation. Then, the DCT is performed on the Y component as the cover image, because the human eye is less sensitive to the luminance Y in YC_bC_r space than other color channels in the RGB space. The SVD is performed on the DCT coefficients obtained from the luminance component Y. The SVs (S matrix) is then divided into $\frac{M}{128} \times \frac{N}{128}$ blocks with each block size of 128 × 128, for an $M \times N$ cover image. The watermark image is pre-processed before embedding into each block using a scaling factor. Finally, the watermarked image is transformed to the spatial domain using the inverse DCT (IDCT). Consider a 3D doctor image of size 256 × 256 for each channel as a cover image [23] and as MRI image of size 128 × 128 as a watermark image [24]. The next two sections depict embedding and extraction algorithms to distinctly define the flow of the proposed technique.

4.1 Embedding Algorithm

The watermark embedding procedure is depicted in Fig. 3, and it is described in detail in the following steps:

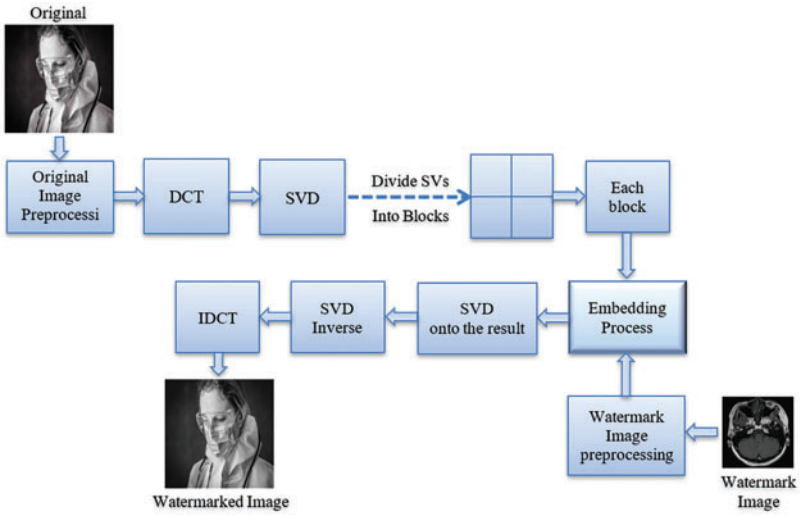


Figure 3: Embedding algorithm

Step 1: The cover image is transformed into YC_bC_r plane.

Step 2: The DCT is applied to the luminance image Y.

Step 3: The SVD is applied to the matrix obtained after applying DCT to obtain:

$$\mathbf{A}_1 = \mathbf{U}_1 \mathbf{S}_1 \mathbf{V}_1^T \tag{6}$$

where $\mathbf{U}_1$ and $\mathbf{V}_1^T$ are the orthonormal unitary matrices of $\mathbf{A}_1$. The term $\mathbf{S}_1$ constitutes the singular values of the matrix $\mathbf{A}_1$.

Step 4: The $\mathbf{S}_1$ component is divided into 128 × 128 blocks.

Step 5: The watermark image is embedded into each block. The embedding process can be defined mathematically as:

$$\mathbf{A}_{1w} = \mathbf{S}_{block} + k.\mathbf{W} \tag{7}$$

where k denotes the scale factor used to control the strength of the watermark to be inserted.

Step 6: The SVD is applied to the result to get $\mathbf{A}_{2w} = \mathbf{U}_2 \mathbf{S}_2 \mathbf{V}_2^T$.

Step 7: The inverse SVD (ISVD) is applied by multiplying the orthogonal matrices $\mathbf{U}_1$ and $\mathbf{V}_1^T$ with the matrix $\mathbf{S}_2$, as given in Eq. (8).

$$\mathbf{A}_{1new} = \mathbf{U}_1 \mathbf{S}_2 \mathbf{V}_1^T \tag{8}$$

Step 8: Finally, the IDCT is applied on $\mathbf{A}_{1new}$ to obtain the watermarked image $\mathbf{A}_w$.

Table 3: Simulation parameters

Parameter	Value
System bandwidth	5 MHz
Cyclic prefix size	20 samples (4 μs)
IFFT/IDCT/IDWT size (M)	512 symbols
Subcarrier spacing	9.765625 kHz (= 5 MHz/512)
Input block size	128 symbols
FFT/DCT/DWT size (N)	128 symbols
Modulation type	16 QAM
Subcarrier mapping methods	Interleaved and localized
Channel models	Pedestrian A and Vehicular A
Channel estimation	Perfect
Equalizer type	MMSE

Table 4: PSNR values of the received decrypted watermarked images over the SC-FDMA system for all studied cases at different SNR values over Pedestrian A channel

	PSNR					
SNR	FFT		DCT		DWT	
	IFDMA	LFDMA	IFDMA	LFDMA	IFDMA	LFDMA
0	9.2737	9.8576	9.3833	9.9545	9.9332	10.7391
3	10.1448	11.1011	10.2839	11.4735	11.7328	13.6521
6	11.4611	13.2059	11.8722	13.7534	15.6754	19.48
9	13.7925	16.5373	14.44	17.7194	22.876	31.6115
12	18.497	22.5944	18.3002	23.9938	44.7993	Inf
15	24.5474	39.7086	24.8822	34.7125	Inf	Inf
18	34.1015	Inf	Inf	Inf	Inf	Inf

4.2 Extraction Algorithm

The watermark extraction procedure is depicted in Fig. 4, and it is described in detail in the following steps:

Step 1: SVD is applied on the watermarked image A_w to obtain A_w^* according to

$$\mathbf{A}_w^* = \mathbf{U}^*\mathbf{S}^*\mathbf{V}^{*T} \tag{9}$$

Step 2: **D** is obtained according to $\mathbf{D} = \mathbf{U}_2\mathbf{S}^*\mathbf{V}_2^T$.

Step 3: **D** is divided into blocks, each with a size of 128×128.

Step 4: The watermark is extracted according to

$$\mathbf{W}^* = (\mathbf{D}_{\mathbf{block}} - \mathbf{S}_{\mathbf{block}})/k \tag{10}$$

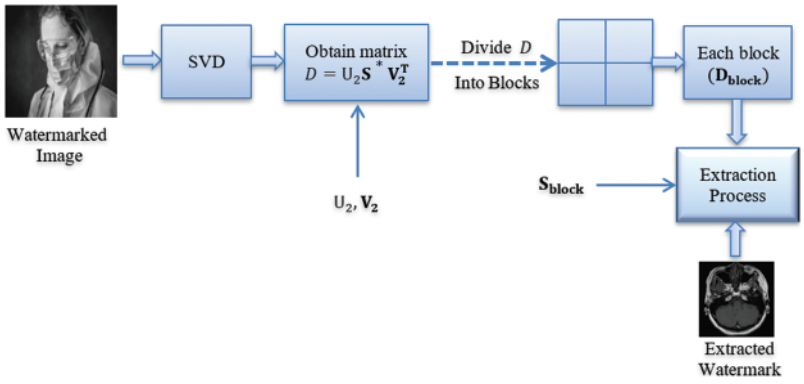


Figure 4: Extraction algorithm

5 Chaos and DNA-Based Ciphering Algorithm

The next two sections depict encryption and decryption algorithms to distinctly define the flow of these algorithms.

5.1 Encryption Algorithm

Chaos-based encryption methods rely on the unpredictable and sensitive nature of chaotic systems. When used for encryption, tiny changes in the initial conditions of the system can produce vastly different outcomes, making chaos a strong tool against cyber-attacks. DNA encoding, inspired by biological DNA sequences, provides a novel way of representing and processing information. The use of chaos and DNA encoding together combines the unpredictability of chaotic systems with the vast encoding potential of DNA sequences, offering a robust encryption method. A comprehensive discussion of this method can be found in [25]. The detailed steps of the encryption based on DNA are explained through the following steps:

Step 1: Eqs. (3) and (11) are used to generate the key image.

$$pixel = [x \times 256] \tag{11}$$

where *pixel* is the pixel value of the key image, x is the iteration value of the PWLCM, and $x \in (0, 1)$. The initial value of Eq. (3) is calculated with the help of Eq. (5).

Step 2: The plain and key images are encoded using DNA rules determined by Eqs. (4) and (12).

$$Rule = [x \times 8] + 1 \tag{12}$$

where *Rule* is the specified rule controlling the encoding progress, and the initial value of Eq. (4) is provided by Eq. (5). The details about DNA rules are shown in Table 1.

According to DNA encoding rules, the gray-scale plain image is encoded using 4 kinds of nucleobases, as it consists of 8 bits. When a plain image of size $M \times N$ is used, the encoded image size will be $4 \times M \times N$.

Step 3: The DNA operation is conducted between the encoded plain image and the encoded key image. Here, the XOR operation is performed row by row until the encoded intermediate image is generated. The size of the encoded intermediate image is $4 \times M \times N$. Details on XOR operation are presented in Table 2.

Step 4: The encoded intermediate image is decoded to obtain a decoded intermediate image. The decoding rule depends on Eq. (12). This step produces a primary cipher image with size $M \times N$.

Step 5: The primary cipher image is rotated by 90° anticlockwise. This step produces a new plain image to be used in the next step.

Step 6: Steps 1 to 4 are repeated to obtain the final cipher image. The encryption based on DNA sequences is illustrated in Figs. 5 and 6.

5.2 Decryption Algorithm

The procedure of acquiring the original image from the encrypted image is the inverse operation with a slight difference as illustrated in the following steps:

Step 1: The cipher image is encoded according to DNA rules as described in Step 2 in the encryption algorithm.

Step 2: The key image is generated and encoded, according to the same Steps 1 and 2 in the encryption algorithm.

Step 3: The encoded key image and the encoded cipher image produced from Steps 1 and 2 are used to generate the intermediate encoded image. The DNA XOR operation described in the encryption process is performed in the deciphering process as it has a symmetric nature as shown in Table 2.

Step 4: The intermediate encoded image generated from Step 3 is decoded.

Step 5: The decoded image obtained from Step 4 is rotated by 90° clockwise.

Step 6: Steps 1 to 4 are repeated to obtain the plain image. The decryption procedure is depicted in Fig. 6.

5.3 FFT-Based SC-FDMA System

The block diagram of the FFT-based SC-FDMA system for encrypted watermarked image transmission is shown in Fig. 7. One base station and U uplink users are assumed. There are totally M subcarriers, and each user is assigned a subset of subcarriers for the uplink transmission. For simplicity, we assume that each user has the same number of subcarriers, N.

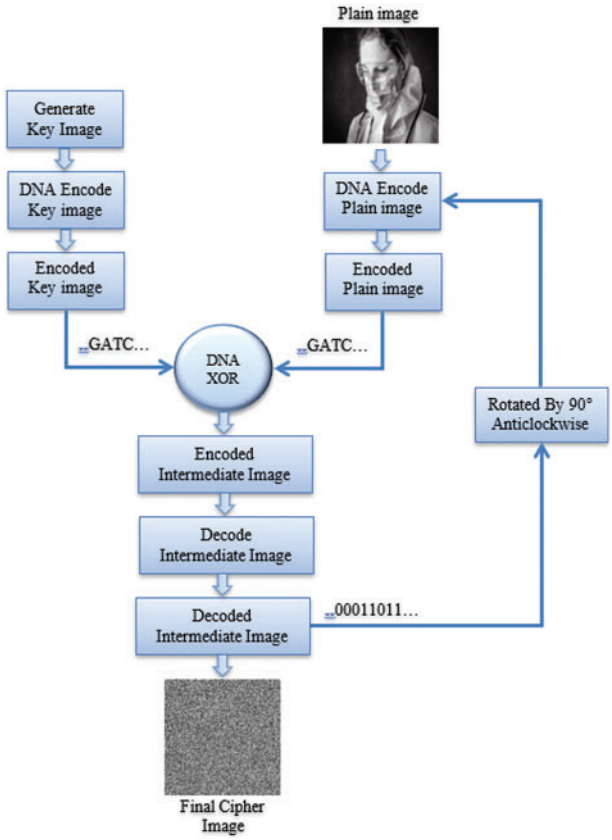


Figure 5: Encryption algorithm

At the transmitter side, the encoded data is transformed into a multilevel sequence of complex numbers in one of several possible modulation formats. The resulting modulated symbols are then grouped into blocks, each containing N symbols and the FFT is performed. The signal after the FFT can be expressed as follows [30–32]:

$$X(k) = \sum_{n=0}^{N-1} x(n)\, e^{\frac{-j2\pi}{N} nk} \tag{13}$$

where N is the input block size, and $x(n)$: $n = 0, \ldots, N-1$ represents the modulated data symbols.

The resulting signal after the IFFT can be given as follows [2]:

$$\overline{x}(m) = \frac{1}{M} \sum_{l=0}^{M-1} \overline{X}(l)\, e^{\frac{j2\pi}{M} ml} \tag{14}$$

where $\overline{X}(l)$: $l = 0, \ldots, M-1$ represents the frequency-domain samples after the subcarriers mapping scheme.

At the receiver side, the Cyclic Prefix (CP) is removed from the received signal and the signal is then transformed into the frequency domain via an M-point FFT.

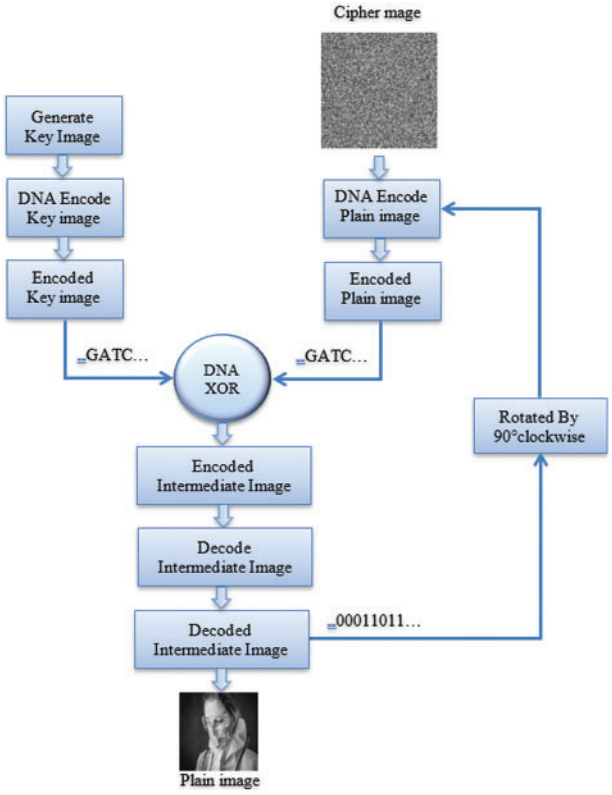


Figure 6: Decryption algorithm

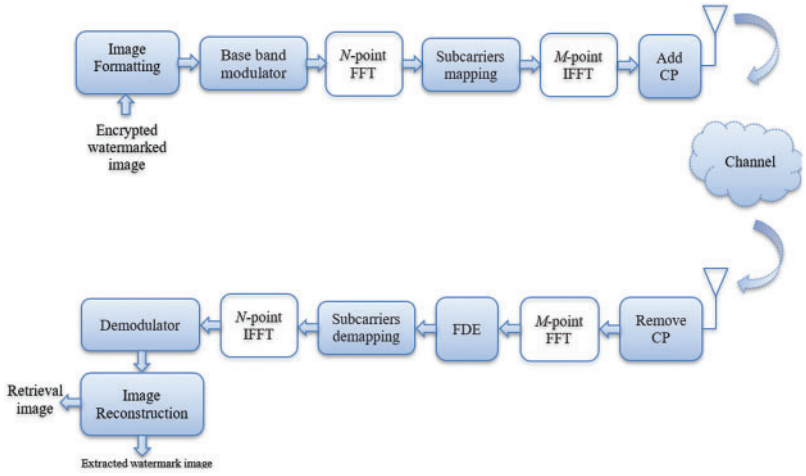


Figure 7: FFT-based SC-FDMA system

5.4 DCT-Based SC-FDMA System

Due to the nature of DCT of energy compaction and real implementation, a DCT-based SC-FDMA system can be used for image communication to avoid the large PAPR and synchronization problems as depicted in Fig. 8 [25]. The spectral energy compaction allows symbol transmission

with low power, which means that the ISI problem will be significantly reduced. In addition, the implementation needs only real arithmetics rather than the complex arithmetics used in the FFT. This reduces the signal processing complexity, and the in-phase/quadrature imbalance, and also makes the system more stable than the FFT-based SC-FDMA system [25,26].

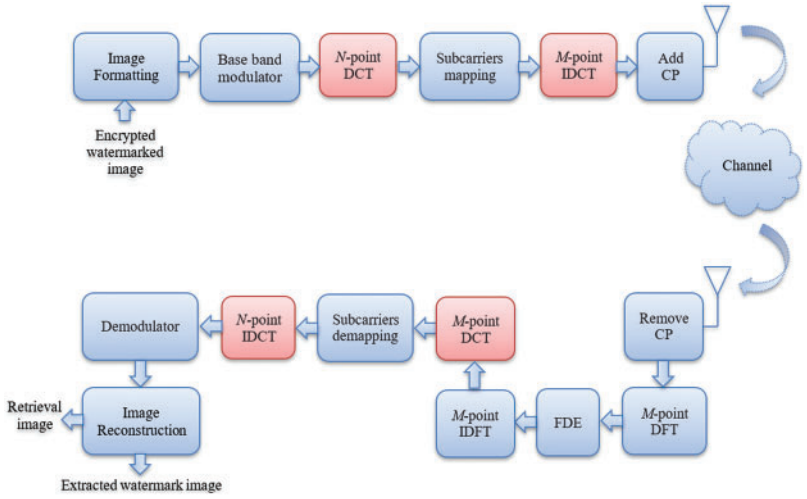


Figure 8: DCT-based SC-FDMA system

Note that although the DCT-based system performs better than the FFT-based system for real-valued functions of input signals, it requires DFT and inverse DFT at the receiver side to achieve one-tap frequency-domain equalization [25].

The minimum F_{Δ}, required to satisfy the orthogonality condition, is $1/2T$. This condition is defined by [26]:

$$\int_0^T \sqrt{\frac{2}{T}}\cos\left(2\pi k F_{\Delta} t\right)\sqrt{\frac{2}{T}}\cos\left(2\pi m F_{\Delta} t\right) d_t = \begin{cases} 1, & k = m \\ 0, & k \neq m \end{cases} \tag{15}$$

A schematic block diagram of the DCT SC-FDMA system is shown in Fig. 8. The signal after the DCT operation can be expressed as follows [26]:

$$X_k = \sqrt{\frac{2}{N}}\beta_k \sum_{n=0}^{N-1} x_n \cos\left(\frac{\pi k\,(2n+1)}{2N}\right) \tag{16}$$

where x_n is the modulated data symbols, and β_k is given by [26–28]:

$$\beta_k = \begin{cases} \dfrac{1}{\sqrt{2}} & k = 0 \\ 1 & k = 1, 2, \ldots\ldots, N-1 \end{cases} \tag{17}$$

After the IDCT, the signal can be expressed as follows:

$$\overline{x}_m = \sqrt{\frac{2}{M}} \sum_{l=0}^{M-1} \overline{X}_l \beta_l \cos\left(\frac{\pi l\,(2m+1)}{2M}\right) \tag{18}$$

where $\overline{X}_l$ is the signal after the subcarrier mapping [29–31].

5.5 DWT-Based SC-FDMA System

Let x_n denote the modulated data symbols. Then, we can describe the signal after the DWT as follows [32–34]:

$$X_k^m = \sum_{n=0}^{N-1} x_n 2^{k/2} \psi\left(2^k - m\right) \tag{19}$$

where $\psi(t)$ denotes the wavelet basis function and X_k^m denotes the wavelet coefficients (See Fig. 9).

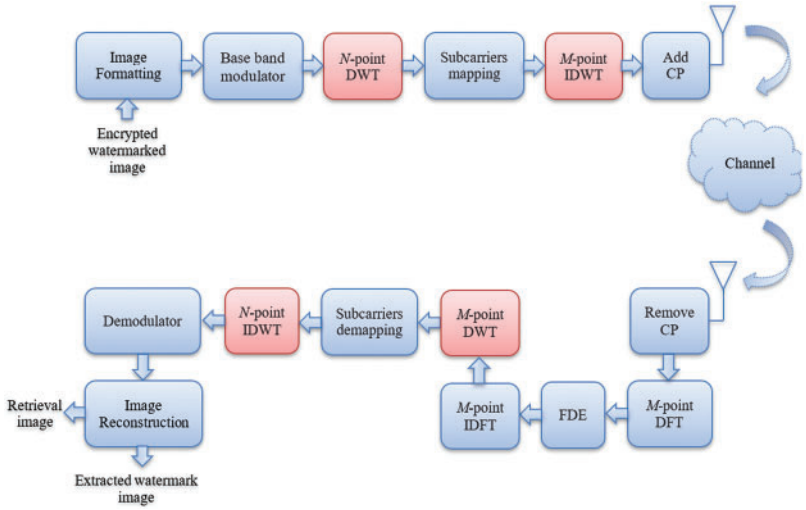


Figure 9: DWT-based SC-FDMA system

6 Simulation Results and Analysis

The process of encrypted watermarked image communication over the SC-FDMA system is studied and analyzed. Different experiments are carried out with different scenarios to evaluate and test the effects of channel models on image quality. The results are presented to assess the performance of different SC-FDMA schemes (FFT SC-FDMA, DCT SC-FDMA and DWT SC-FDMA) over Pedestrian A and Vehicular A channel models. The MMSE equalizer is considered in this study. In addition, two subcarrier mapping schemes, namely localized and interleaved schemes, are studied.

6.1 Simulation Parameters

Experimental results have been obtained using MATLAB simulator to study how efficient the different versions of SC-FDMA are for the transmission of encrypted watermarked images. The details of the simulation parameters are given in Table 3 [35–37].

6.2 Simulation Scenario and System Block Diagram

A block diagram is given in Fig. 10 for the image communication system. The system operation has five stages [37]:

- ***The first stage:*** The watermark image is embedded in the cover image using the embedding process explained earlier in Section 3.1.

- ***The second stage:*** The watermarked image is now encrypted using the encryption algorithm explained earlier in Section 4.1.
- ***The third stage:*** The encrypted watermarked image is now transmitted through either FFT SC-FDMA, DCT SC-FDMA or DWT SC-FDMA system. The MMSE equalizer is considered in the simulation. One of the two subcarrier mapping schemes, either localized or interleaved, is considered. Two different wireless channel models, namely Pedestrian A and Vehicular A, are investigated and compared in this evaluation.
- ***The fourth stage*:** The received encrypted watermarked image at the other end of the wireless channel is passed through the SC-FDMA receiver, and then decrypted using the decryption algorithm explained earlier in Section 3.2.
- ***The fifth stage*:** Finally, the original image is retrieved, and the watermark is extracted from the decrypted watermarked image using the watermark extraction process implemented in Section 4.2.

6.2.1 Subcarrier Mapping Schemes: Localized vs. Interleaved

Subcarrier mapping schemes play an essential role in the operation of SC-FDMA systems, affecting both the system performance and the computational complexity. Here, we briefly discuss the rationale behind choosing the localized and interleaved schemes for comparison and differentiate between them based on their inherent advantages and disadvantages:

➢ ***Localized Mapping:***

- ***Advantages:***
  - ◯ *Simplicity:* One of the main advantages of the localized mapping scheme is its simplicity. The subcarriers are allocated contiguously to each user, making the allocation straightforward.
  - ◯ *Channel Adaptation:* Due to contiguous allocation, localized mapping can exploit the channel frequency selectivity. When used in conjunction with adaptive modulation and coding, it can provide significant performance improvements over frequency-selective channels.

- ***Disadvantages:***
  - ◯ Localized mapping might result in a higher PAPR, which can be a drawback for power-limited systems.

➢ ***Interleaved Mapping:***

- ***Advantages:***
  - ◯ *Diversity:* This scheme offers frequency diversity as it allocates subcarriers in a non-contiguous manner. This scattered allocation can be beneficial in flat-fading scenarios, providing a more uniform performance across the frequency spectrum.
  - ◯ *Reduced PAPR:* Interleaved mapping generally results in a lower PAPR compared to localized mapping, which can lead to power savings.

- ***Disadvantages:***
  - ◯ *Complexity:* The non-contiguous allocation makes the system somewhat more complex, both in terms of subcarrier allocation and signal processing.

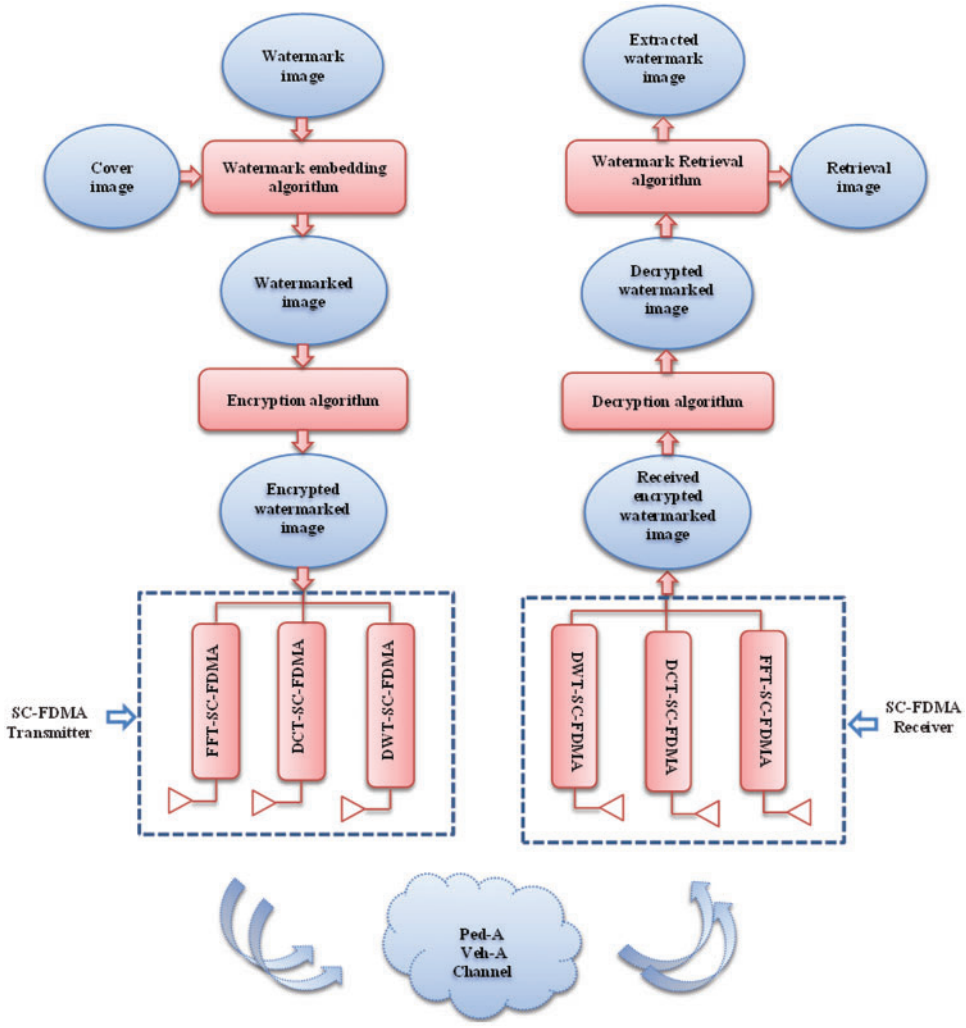


Figure 10: System block diagram

In the context of our study, comparing these two schemes allows us to understand better how they impact the transmission of digital images over different channel models. Considering the unique characteristics of image signals and the challenges associated with their transmission over wireless channels, examining the performance of these schemes is crucial to determining the optimal choice for specific scenarios. By offering insights into the trade-offs associated with each mapping scheme, we aim to provide a comprehensive guide for practitioners and researchers in the field, aiding in making informed decisions when setting up SC-FDMA systems for image transmission tasks.

6.2.2 Channel Models and Modulation Technique: Rationale

➢ ***Channel Models: Pedestrian A and Vehicular A***

The decision to consider both Pedestrian A and Vehicular A channel models stems from the real-world scenarios that they represent.

- **Pedestrian A Model:** This model is primarily designed to emulate scenarios where the primary source of signal impairment comes from time dispersion caused by multi-path propagation. Given the increase in pedestrian users of mobile communication, especially in urban environments, it is crucial to understand how image transmission behaves in such conditions.
- **Vehicular A Model:** Vehicular scenarios, on the other hand, introduce higher doppler shifts due to the high mobility involved. Given the rise in vehicle-to-vehicle and vehicle-to-infrastructure communications, ensuring secure image transmissions in such environments becomes essential.

By contrasting the performance of our algorithm across these two distinct scenarios, we aim to provide a comprehensive evaluation that caters to a broader range of real-world applications.

➢ ***Quadrature Amplitude Modulation***

QAM was chosen as the modulation technique due to its wide adoption in wireless communication and its ability to transmit a larger amount of data for a given bandwidth, making it highly efficient. With the increase in demand for data-intensive tasks such as image transmission, QAM provides a good balance between bandwidth efficiency and performance. In our study, understanding how QAM interacts with our proposed cybersecurity algorithm can give valuable insights into potential practical deployments.

In essence, our choice of channel models and modulation technique is rooted in the aspiration to make our findings as applicable and relevant as possible to the evolving landscape of wireless communication. By considering real-world scenarios and widely-adopted modulation techniques, we aim to bridge the gap between academic research and practical implementation.

6.3 PSNR-Based Image Communication Assessment

The PSNR can be mathematically calculated with Eq. (20) [5].

$$PSNR\,(dB) = 10\log\left(\frac{P^2{}_{Max}}{MSE}\right) = 20log\left(\frac{P_{Max}}{\sqrt{MSE}}\right) \tag{20}$$

where P_{Max} is the highest pixel value given as $P_{Max} = 2^b - 1$, and b is the number of bits per sample. The MSE is calculated mathematically with Eq. (21) [5].

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[f\,(i,j) - f'\,(i,j)]^2 \tag{21}$$

where $f\,(i,j)$ is the original cover image and $f'(i,j)$ is the received decrypted watermarked image.

The PSNR performance of the system is evaluated for different SNRs. The PSNR is evaluated between the decrypted watermarked image at the receiver and the original image. It is measured for performance assessment for all different studied schemes: DWT SC-FDMA, DCT SC-FDMA, and FFT SC-FDMA, an MMSE equalizer and two subcarrier mapping schemes (localized and interleaved). The PSNR performance of all schemes is studied over two different channel models: Pedestrian A and Vehicular A.

6.3.1 PSNR Performance over Pedestrian A Channel

For the Pedestrian A channel, Fig. 11 shows that the DWT SC-FDMA scheme outperforms the DCT SC-FDMA and FFT SC-FDMA schemes. The DCT SC-FDMA and FFT SC-FDMA have approximately the same performance. The DWT-LFDMA outperforms the DWT-IFDMA.

Generally, the DWT-LFDMA has the best performance. Generally, For the Pedestrian A channel, the DWT-LFDMA is the best of all studied cases.

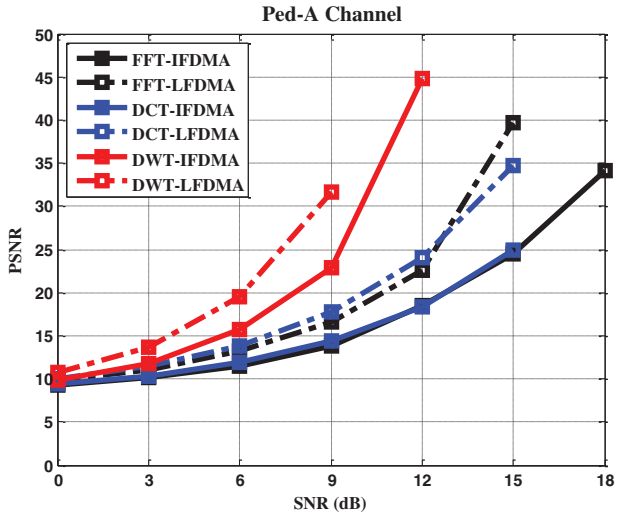


Figure 11: PSNR performance of FFT/DCT/DWT-based IFDMA and LFDMA systems over Pedestrian A channel, with MMSE equalizer

6.3.2 PSNR Performance over Vehicular A Channel

For the Vehicular A channel, Fig. 12 shows that the DCT-LFDMA has the best performance. The DWT-IFDMA and the DWT-LFDMA have a satisfactory performance unlike the DCT-IFDMA and FFT-IFDMA, which give the worst performance for the Vehicular A channel. Generally, for the Vehicular A channel, the DCT-LFDMA is by far the best performance of all studied cases.

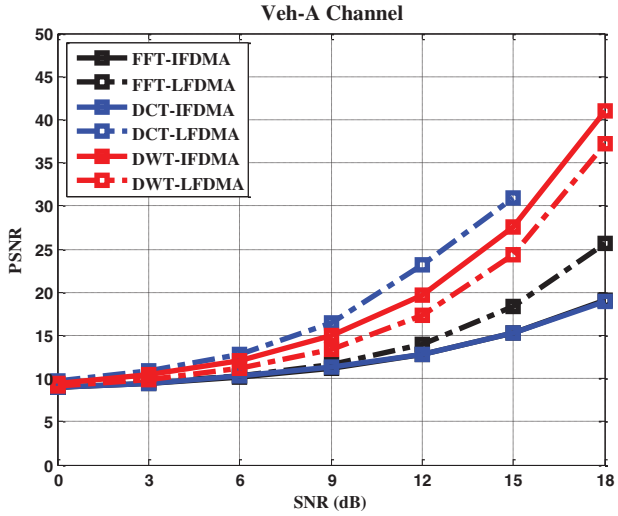


Figure 12: PSNR performance of FFT/DCT/DWT-based IFDMA and LFDMA systems over Vehicular A channel, with MMSE equalizer

The complete set of results of all simulation experiments is tabulated in Tables 4 and 5. These tables provide the PSNR *vs.* channel SNR in all simulation scenarios. It is noticed that as SNR is increased, there is an improvement in the PSNR values for the decrypted watermarked images. A PSNR value approaching infinity indicates that the MSE between the original and the decrypted watermarked images is zero, i.e., the original image quality is achieved in the decrypted watermarked image.

For Pedestrian A channel, it can be noticed from Table 4 that the PSNR gets its maximum value at a channel SNR equal to 12 dB for the DWT-LFDMA scheme. On the other hand, the PSNR gets its maximum at a channel SNR equal to 15 dB for the DWT-IFDMA scheme. It can be noticed that DCT-IFDMA, DCT-LFDMA and the FFT-LFDMA schemes have approximately the same performance over the Pedestrian A channel, as they reach their maximum PSNR at a channel SNR equal to 18 dB. The FFT-LFDMA has the worst performance compared to all the studied cases. The DWT-LFDMA achieves the best performance over the Pedestrian A channel as an SNR of 12 dB only is required to transmit images with high quality.

For the Vehicular A channel, it can be noticed from Table 5 that PSNR gets the optimum value at a channel SNR equal to 18 dB for the DCT-LFDMA scheme. The PSNR gets 40.961 and 37.1968 dB values at a channel SNR equal to 18 dB for the DWT-IFDMA and DWT-LFDMA schemes, respectively, which are satisfactory values to transmit images over Vehicular A channel. It can be noticed also that the worst cases are for the FFT-IFDMA and DCT-IFDMA.

Table 5: PSNR values of the received decrypted watermarked image over the SC-FDMA system for all studied cases at different SNR values over Vehicular A channel

	PSNR					
SNR	FFT		DCT		DWT	
	IFDMA	LFDMA	IFDMA	LFDMA	IFDMA	LFDMA
0	8.956	9.011	8.9635	9.7827	9.4543	9.1511
3	9.4913	9.5414	9.4979	10.8532	10.418	9.9137
6	10.2084	10.3618	10.2539	12.7396	12.0783	11.1851
9	11.203	11.695	11.3153	16.484	14.9498	13.3781
12	12.7385	13.9609	12.8617	23.1515	19.6402	17.3892
15	15.2377	18.3756	15.2698	30.8899	27.5452	24.3258
18	19.0933	25.5879	18.8692	Inf	40.961	37.1968

6.4 Image Communication Assessment Based on Bit Error Rate

In digital transmission, the BER is a key parameter that is used in assessing the system performance in the transmission of digital data from one location to another. There is a possibility of errors being introduced into the system, when data is transmitted over the link. As a result, it is necessary to evaluate the performance of the system, and the BER provides an ideal way in which this can be achieved. The BER reflects the performance of the whole system including the transmitter, receiver and the medium between them [30].

The BER is the number of bits with errors divided by the total number of bits that have been transmitted, received or processed over a given period [30]. That is:

$$BER = \frac{Number\ of\ bits\ with\ error}{Total\ number\ of\ bits\ sent} \tag{22}$$

The BER is decreased with the increase in the channel SNR, which means that the BER is inversely proportional to channel SNR. The BER performance of the different schemes is shown in Figs. 13 and 14.

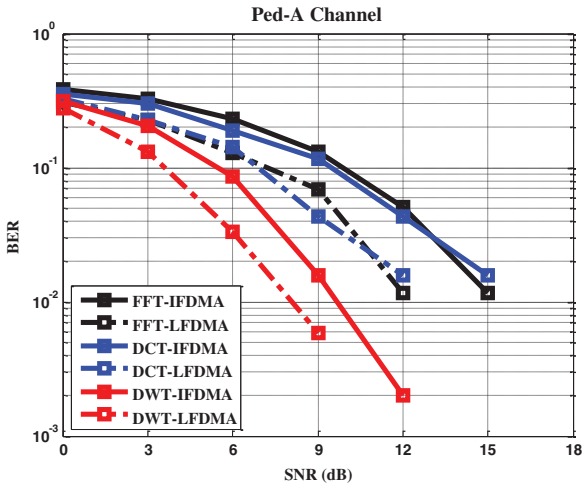


Figure 13: BER performance of FFT/DCT/DWT-based IFDMA and LFDMA schemes over pedestrian A channel with MMSE equalizer

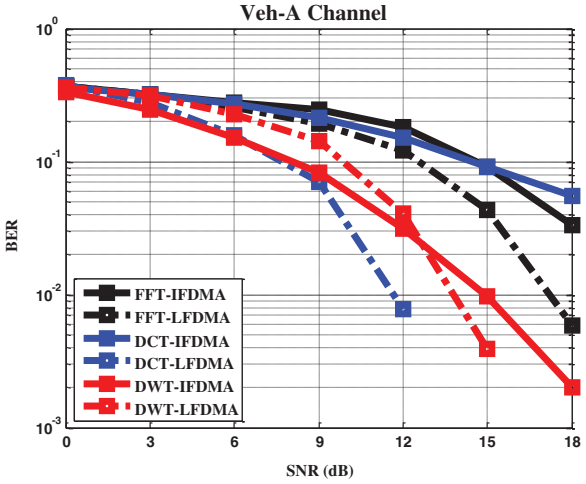


Figure 14: BER performance of FFT/DCT/DWT-based IFDMA and LFDMA schemes over vehicular A channel with MMSE equalizer

6.4.1 BER Performance over Pedestrian A Channel

Fig. 13 demonstrates the BER performance of all the studied cases over the Pedestrian A channel with MMSE equalizers. Fig. 13 indicates that the DWT SC-FDMA has lower BER than the FFT SC-FDMA and DCT SC-FDMA schemes. The DWT-LFDMA just needs 12 dB SNR for the BER to be zero. It can be noticed that DWT-IFDMA, DCT-LFDMA and the FFT-LFDMA schemes need larger SNR values of up to 15 dB to reach the zero BER value. DCT-IFDMA and the FFT-IFDMA need an SNR value equal to 18 dB for a BER equal to zero.

The complete set of results of all simulation experiments is tabulated in Table 6. Table 6 provides the BER *vs.* channel SNR in all simulation scenarios over the Pedestrian A channel. It is clear that over the Pedestrian A channel, the DWT-LFDMA is by far the best considering all studied cases as it reaches a BER of zero value at the smallest value of SNR of 12 dB. It is also observed that the localized subcarrier mapping scheme has better performance than that of the interleaved subcarrier mapping scheme.

6.4.2 BER Performance over Vehicular A Channel

Fig. 14 shows the BER performance over the Vehicular A channel for the MMSE equalizer. Fig. 14 indicates that the DCT-LFDMA scheme gives lower BER than the DCT-IFDMA, FFT-SCFDMA and DWT-SCFDMA schemes. The DCT-LFDMA gets a BER value of zero at an SNR value equal to 15 dB. The DWT-LFDMA needs 18 dB SNR for a BER of zero. DCT-IFDMA and FFT-IFDMA have the worst BER values. The complete set of results of all simulation experiments is tabulated in Table 7.

Table 6: BER values of the received decrypted watermarked images with the SC-FDMA system for all studied cases at different SNR values over Pedestrian A channel

	BER					
SNR	FFT		DCT		DWT	
	IFDMA	LFDMA	IFDMA	LFDMA	IFDMA	LFDMA
0	0.3809	0.3047	0.3555	0.3262	0.3105	0.2773
3	0.3242	0.2266	0.3027	0.2266	0.2051	0.1309
6	0.2305	0.1289	0.1895	0.1426	0.0859	0.0332
9	0.1309	0.0684	0.1152	0.043	0.0156	0.0059
12	0.0508	0.0117	0.043	0.0156	0.002	0
15	0.0117	0	0.0156	0	0	0
18	0	0	0	0	0	0

Table 7 provides the BER *vs.* channel SNR in all simulation scenarios over the Vehicular A channel. It is clear that over the Vehicular A channel, the DCT-LFDMA is by far the best of all studied cases as it reaches a BER of zero value at the smallest value of SNR of 15 dB. On the other hand, other schemes require higher SNR values of 18 dB or above to reach the BER of zero.

Table 7: BER values of the received decrypted watermarked images with the SC-FDMA system for all studied cases at different SNR values over Vehicular A channel

SNR	BER					
	FFT		DCT		DWT	
	IFDMA	LFDMA	IFDMA	LFDMA	IFDMA	LFDMA
0	0.3652	0.3711	0.3613	0.375	0.3301	0.3594
3	0.3203	0.3223	0.3164	0.2773	0.2441	0.3145
6	0.2773	0.2559	0.2695	0.1582	0.1523	0.2285
9	0.2441	0.1914	0.2148	0.0703	0.082	0.1426
12	0.1797	0.1211	0.1523	0.0078	0.0313	0.041
15	0.0918	0.043	0.0918	0	0.0098	0.0039
18	0.0332	0.0059	0.0547	0	0.002	0

6.5 Image Communication Assessment Based on Correlation Coefficients (C_r)

The correlation coefficient of two images is given as follows:

$$C_r = \frac{\sum_m \sum_n (A_{mn} - \overline{A})(B_{mn} - \overline{B})}{\sqrt{((\sum_m \sum_n (A_{mn} - \overline{A})^2)(\sum_m \sum_n (B_{mn} - \overline{B})^2)}} \tag{23}$$

where $\overline{A}$ is the mean of A, and $\overline{B}$ is the mean of B.

At the receiver side, the watermark is extracted from the decrypted watermarked image. The correlation performance is analyzed by considering all different studied schemes over Pedestrian A and Vehicular A channels. Figs. 15 and 16 show the bar chart that reveals the plot of the correlation coefficient between original and extracted watermarks *vs.* SNR for all the studied cases in this simulation.

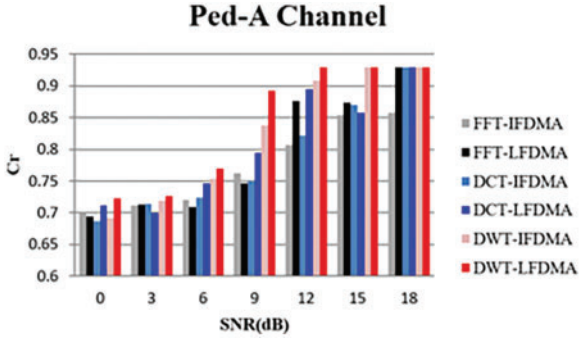


Figure 15: Correlation coefficient performance of FFT/DCT/DWT-based IFDMA and LFDMA systems over Pedestrian A channel with MMSE equalizer

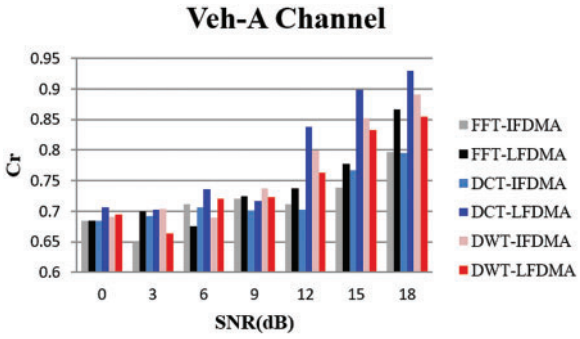


Figure 16: Correlation coefficient performance of FFT/DCT/DWT-based IFDMA and LFDMA systems over Vehicular A channel with MMSE equalizer

6.5.1 Correlation Performance over Pedestrian A Channel

Fig. 15 demonstrates the correlation performance of all the studied cases over the Pedestrian A channel with MMSE equalizer. Fig. 15 indicates that the DWT SC-FDMA scheme achieves better correlation values than those of the FFT SC-FDMA and DCT SC-FDMA schemes. The localized subcarrier mapping achieves better correlation values than those of the interleaved subcarrier mapping scheme.

The complete set of results of all simulation experiments is tabulated in Table 8. For Pedestrian A channel, Table 8 demonstrates that the DWT-LFDMA is by far the best of all studied cases as it gives the optimum correlation coefficient value of $C_r = 0.929$ at a value of SNR equal to 12 dB. It is also observed that the localized subcarrier mapping scheme has a better performance than that of the interleaved subcarrier mapping scheme.

Table 8: Correlation coefficient values of the received decrypted watermarked images with the SC-FDMA system for all studied cases at different SNR values over Pedestrian A channel

	C_r					
SNR	FFT		DCT		DWT	
	IFDMA	LFDMA	IFDMA	LFDMA	IFDMA	LFDMA
0	0.7006	0.6942	0.6872	0.7113	0.6919	0.7224
3	0.7118	0.7126	0.7146	0.6987	0.7186	0.7266
6	0.7203	0.7095	0.7242	0.7464	0.7532	0.7702
9	0.7624	0.7465	0.7503	0.7943	0.8382	0.892
12	0.8067	0.876	0.8218	0.8944	0.9089	0.929
15	0.8541	0.8736	0.8699	0.857	0.929	0.929
18	0.8581	0.929	0.929	0.929	0.929	0.929

6.5.2 Correlation Coefficient Performance over Vehicular A Channel

Fig. 16 shows the correlation coefficient performance over the Vehicular A channel for MMSE equalizer. Fig. 16 indicates that DCT-LFDMA achieves better correlation values than those of the FFT-SCFDMA and DWT-SCFDMA, particularly with the localized subcarrier mapping.

The complete set of results of all simulation experiments is tabulated in Table 9. Table 9 demonstrates that for the Vehicular A channel, the DCT-LFDMA is by far the best of all studied cases, as it gives the optimum correlation coefficient value of $C_r = 0.929$ at an 18 dB value of SNR.

Table 9: Correlation coefficient values of the received decrypted watermarked images with the SC-FDMA system for all studied cases at different SNR values over Vehicular A channel

	C_r					
SNR	FFT		DCT		DWT	
	IFDMA	LFDMA	IFDMA	LFDMA	IFDMA	LFDMA
0	0.6838	0.6849	0.6843	0.7058	0.6904	0.6941
3	0.6502	0.7004	0.6916	0.702	0.7037	0.6639
6	0.7109	0.6752	0.706	0.7365	0.6898	0.72
9	0.7205	0.7244	0.7011	0.7164	0.7369	0.723
12	0.7119	0.7371	0.703	0.838	0.7994	0.7634
15	0.7383	0.7769	0.7664	0.8984	0.8517	0.8334
18	0.7966	0.8665	0.7955	0.929	0.8903	0.8546

6.6 Imperceptibility Analysis

To validate the watermark embedding into the original image, perceptual quality analysis is considered. In a good embedding technique, the watermarked image should be visibly identical to the original image. The perceptual transparency or imperceptibility of the proposed technique is measured with PSNR. Watermarked and original images should be very similar. Higher PSNR values indicate higher imperceptibility and less distortion.

A 3D image of size 256 × 256 has been considered to be an original image in this simulation experiment. Figs. 17a and 17b show the original image and its histogram. Figs. 17c and 17d show the watermarked image and its histogram and Figs. 17c and 17d show the encrypted watermarked image and its histogram, respectively.

6.6.1 Imperceptibility Analysis over Pedestrian A Channel

To analyze the imperceptibility or perform visual inspection of the decrypted watermarked images over all different studied schemes over Pedestrian A channel, a value of SNR = 12 dB is considered as shown in Fig. 18. It is clear that the quality of the received decrypted watermarked image with the DWT-LFDMA system is better than those of the FFT SC-FDMA, DCT SC-FDMA, and the other case of the DWT SC-FDMA systems. The transparency of the received images obtained through DWT-LFDMA is by far the best of all studied cases.

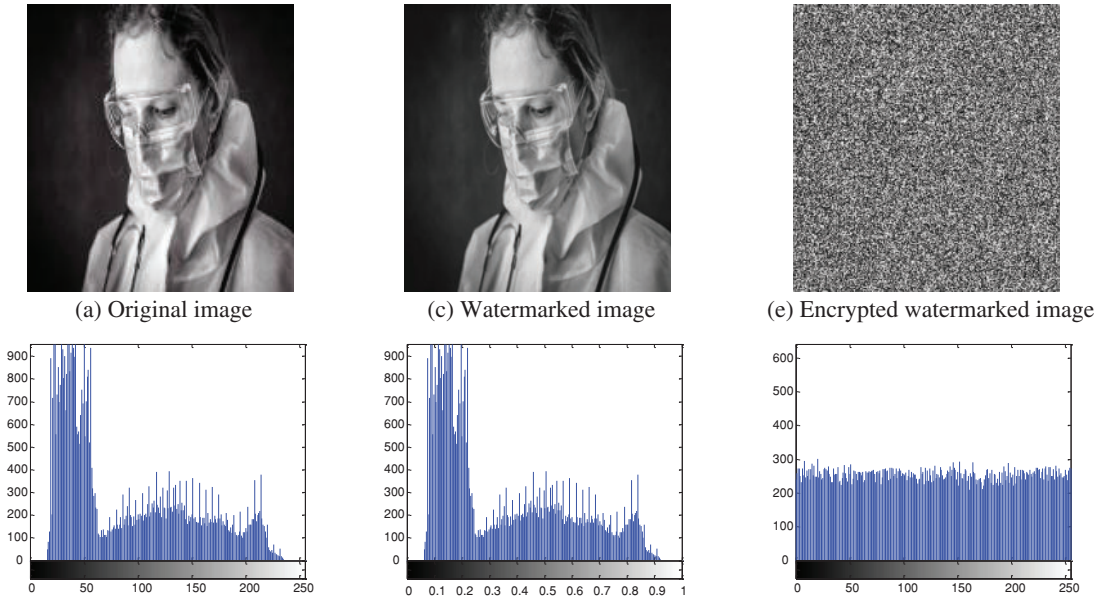


Figure 17: Original, watermarked and encrypted watermarked images and their histograms

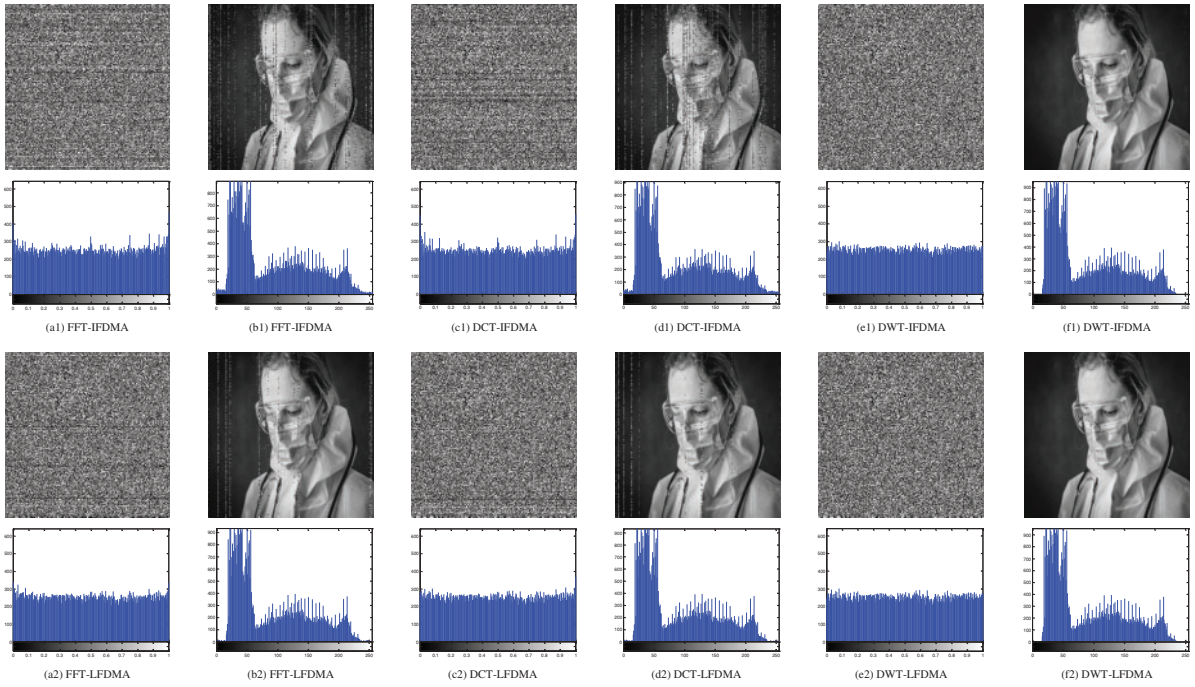


Figure 18: Simulation results of encrypted/decrypted watermarked images and their histograms at SNR = 12 dB over Pedestrian A channel for different schemes

6.6.2 Imperceptibility Analysis over Vehicular A Channel

To analyze the imperceptibility or perform visual inspection of the decrypted watermarked images over all different studied schemes over the Vehicular A channel, a value of SNR = 18 dB is considered as shown in Fig. 19. It is clear that the quality of the received decrypted watermarked image using the DCT-LFDMA scheme is better than those of the FFT SC-FDMA, DWT SC-FDMA and the other case of DCT-SCFDMA. The transparency of the received images obtained through the DCT SC-FDMA scheme is the best over the vehicular A channel for the localized subcarrier mapping scheme (DCT-LFDMA).

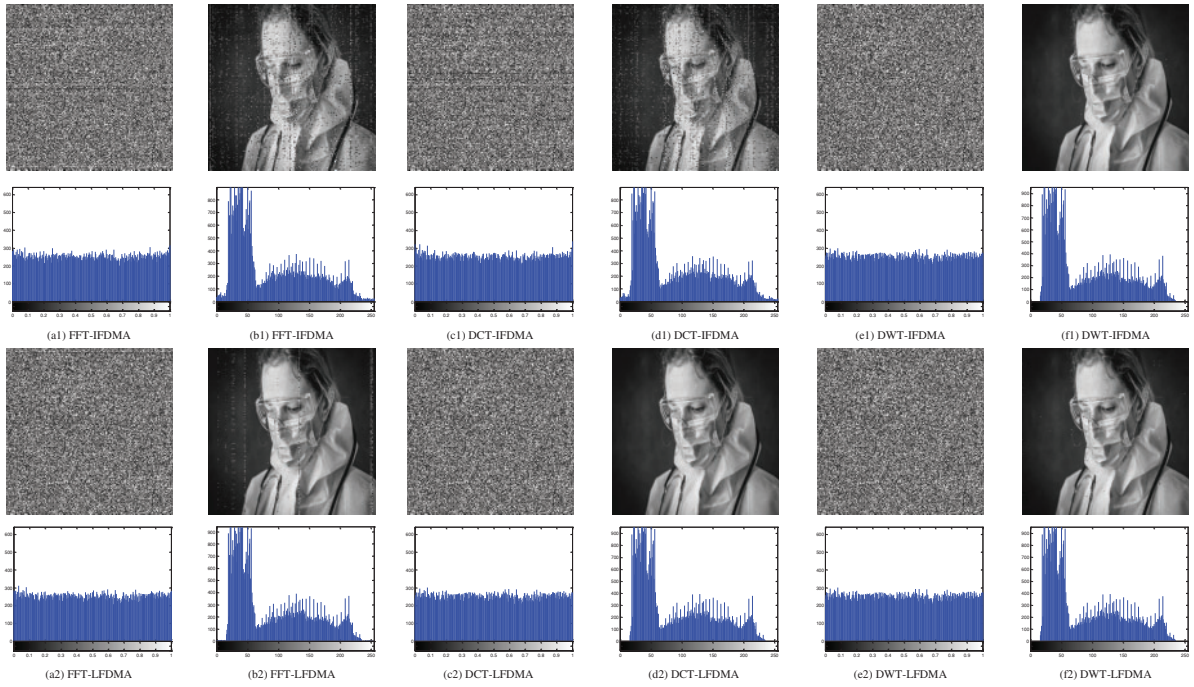


Figure 19: Simulation results of encrypted/decrypted watermarked images and their histograms at SNR = 18 dB over Vehicular A channel for different schemes

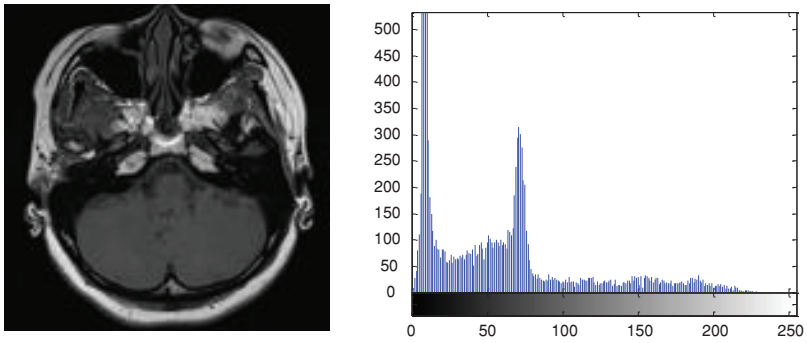
6.7 Robustness Analysis

The robustness of extracted watermarks is evaluated using correlation coefficients C_r between the original and extracted watermark image at the receiver. As mentioned earlier, the optimum case produces C_r values close to unity, which means a great similarity between the original and the extracted watermarks. Fig. 20 shows the original watermark image used in the simulation experiments and its histogram.

6.7.1 Robustness Analysis over Pedestrian A Channel

To see whether the watermark has been extracted exactly and to study the robustness of the extracted watermark image at the receiver side of all different studied schemes over Pedestrian A channel, a value of SNR = 12 dB is chosen as shown in Fig. 21. From comparative analysis depicted in Fig. 21, it is quite obvious that the quality of the extracted watermark image using the DWT-LFDMA scheme is better than those of the FFT SC-FDMA and DCT SC-FDMA and the other cases of DWT

SC-FDMA schemes. The DWT-LFDMA system delivers the best correlation value of $C_r = 0.929$, which signifies higher robustness than those of other schemes.



(a) Watermark image (b) Histogram of watermark image

Figure 20: Original watermark image and its histogram

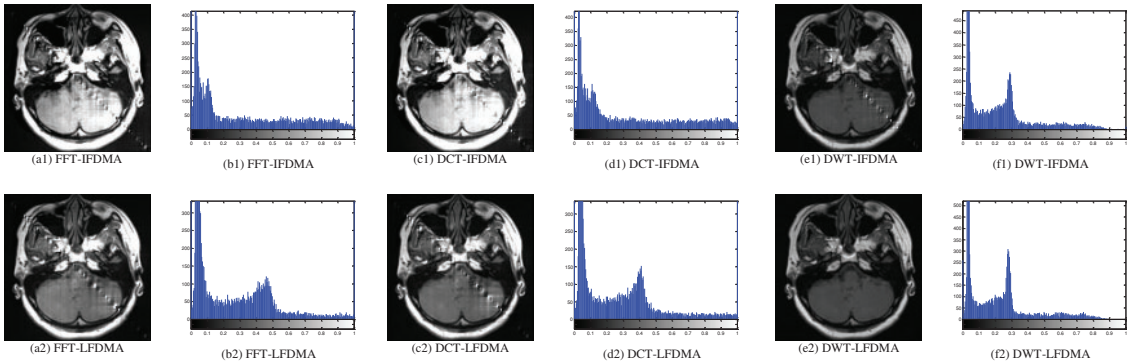


Figure 21: Simulation results of extracted watermark images and their histograms at SNR = 12 dB over Pedestrian A channel for different schemes

6.7.2 Robustness Analysis over Vehicular A Channel

To see whether the watermark has been extracted exactly and to study the robustness of extracted watermark images at the receiver side for all different studied schemes over Vehicular A channel, a value of SNR = 16 dB is chosen as shown in Fig. 22. From comparative analysis depicted in Fig. 22, it is quite obvious that the quality of the extracted watermark image using the DCT-LFDMA scheme is better than those of the FFT SC-FDMA and DWT SC-FDMA and the other cases of DCT SC-FDMA schemes. The DCT-LFDMA delivers the best correlation value of $C_r = 0.929$, which signifies higher robustness for the localized subcarrier mapping method (DCT-LFDMA).

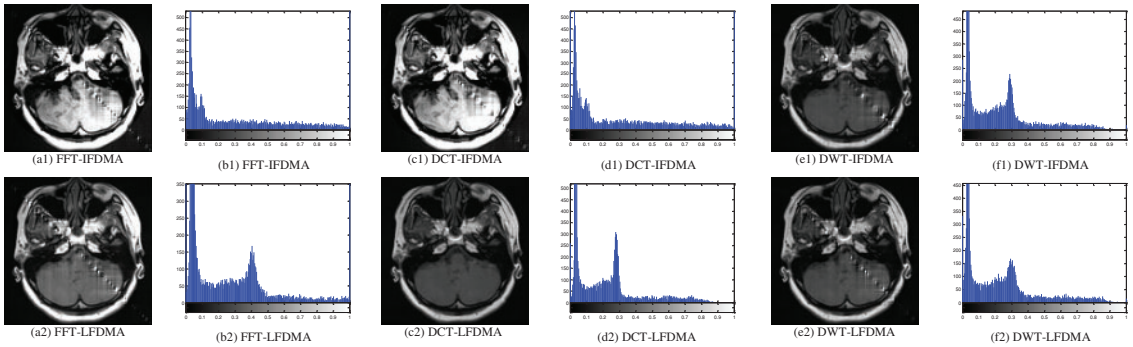


Figure 22: Simulation results of extracted watermark images and their histograms at SNR = 18 dB over Vehicular A channel for different schemes

6.8 Performance Analysis in Terms of Histograms

6.8.1 Histogram Overview

A histogram is a graphical illustration of the pixel levels of an image. It is the representation of variation in the perception of a tone. It describes the distribution of gray levels of a given image [31]. The x-axis represents the tonal variations of the image and the y-axis represents the number of pixels of a particular tone [32].

6.8.2 Histogram Analysis

The histograms of the original, watermarked and encrypted watermarked images are shown in Figs. 17b, 17d and 17f, respectively. It is quite obvious that the original and watermarked image histograms are similar to each other. Fig. 17f shows that the histogram of the encrypted watermarked image is uniform.

To analyze the histograms of the received encrypted and decrypted (retrieved) watermarked images over all different studied schemes over Pedestrian A channel and Vehicular A channel, values of SNR = 12 dB and SNR = 18 dB are considered as shown in Figs. 18 and 19, respectively. It is quite evident from these figures that the received encrypted watermarked images still maintain their uniform histogram nature, and this makes the schemes stronger against different attacks. It is also evident that decrypted (retrieved) watermarked images are similar to the original and watermarked images, which means that the histogram gives a clear significance that the decryption has produced the original image.

The histograms of the extracted watermark images at the receiver side for all different studied schemes over Pedestrian A channel and Vehicular A channel at values of SNR = 12 dB and SNR = 18 dB are considered as shown in Figs. 21 and 22, respectively. It is quite evident from these figures compared with Fig. 20 that the extracted watermark image is highly correlated with the original watermark image, which means that the watermark has been extracted significantly at the receiver side.

6.9 Comparison with Previous Works

To provide a clearer understanding of the advances and distinctions of our proposed method, we present a comparative study between our work and previous related methodologies in the domain

of image transmission over SC-FDMA systems. Table 10 offers a side-by-side comparison based on various crucial metrics and parameters.

Table 10: Comparison with previous works

Criteria	Our method	[6]	[7]	[15]
Algorithm/technique	DWT-SC-FDMA/DCT-SC-FDMA	DWT	DCT	SVD
Watermarking & encryption	DCT-SVD & Chaos-DNA encoding	DCT-SVD	2D Chaos	DNA
Channel models tested	Pedestrian A & Vehicular A	Vehicular A	Pedestrian A	Vehicular A
Reconstructed image quality (PSNR (dB))	32.15	20.13	22.17	21.53
Robustness against errors/attacks	High robustness to all common multimedia attacks	Week robustness	Moderate robustness	Week robustness
Time complexity	2.3 s	6.8 s	5.7 s	5.2 s

From the table, it becomes evident that our proposed method is a holistic tool by integrating advanced watermarking and encryption techniques, ensuring both the security and quality of transmitted images. Moreover, the robustness of our approach against potential transmission errors and attacks further emphasizes the relevance and novelty of our research in the context of SC-FDMA-based image communication systems.

6.10 Complexity Analysis of the Proposed Algorithms

In this section, we present a comprehensive complexity analysis of the various algorithms introduced in our paper. This includes the DCT-SVD-based watermarking, chaos and DNA-based image encryption, and the linear MMSE equalizer. The intention behind this analysis is to provide insights into the computational demands of each algorithm, aiding potential implementers in understanding the trade-offs involved in their application.

- ***DCT-SVD-Based Watermarking:***
- ***Time Complexity:***
- Discrete Cosine Transform (DCT): Since we employ a 2D-DCT on images of size $M \times N$, the time complexity is of O($N\ log\ (MN)$).
- Singular Value Decomposition (SVD): On a square matrix of size $M \times M$, SVD complexity is of O(M^3).

Thus, the overall complexity of DCT-SVD watermarking is of O($MN\log\ (MN) + M^3$).

- ***Space Complexity:*** The space complexity remains of O(MN) as we only need to store the transformed image and singular values.
- ***Chaos and DNA-Based Image Encryption:***

- ***Time Complexity:***
- Chaos encryption typically has a linear time complexity, O(MN), for an image of size $M \times N$.
- DNA encoding: Since each pixel undergoes a specific DNA sequence conversion, its time complexity is also of O(MN).

Thus, the combined time complexity is of O($2MN$), which can be approximated to O(MN) for large images.

- ***Space Complexity:*** The space complexity is of O(MN), which is needed for the DNA-encoded and encrypted image.
- ***MMSE Linear Equalizer:***
- ***Time Complexity:*** Considering the matrix inversion operation required for the MMSE equalizer, if the matrix is of size $M \times M$, the complexity is of O(M^2) using the best-known matrix multiplication algorithms.
- ***Space Complexity:*** Since we need to store the inverse matrix, the space complexity is O(M^2).
- ***Conclusion of Complexity Analysis:***

When considering the implementation of our algorithms in real-world scenarios, the time complexities indicate the computational demand for processing each image, with the MMSE equalizer being the most computationally intensive due to matrix inversion. However, in terms of space requirements, all algorithms only need to allocate space proportional to the image size, making them feasible for most modern systems.

It is also essential to consider that these complexities provide a worst-case scenario. In many practical applications and with the assistance of optimized libraries and hardware, the computational demands may be significantly reduced.

We believe that understanding these complexities will guide practitioners in choosing the appropriate systems and resources when implementing the proposed cybersecurity algorithms for image transmission over advanced communication channel models.

6.11 Discussions

This section delves deeper into the broader implications, challenges, and potential future avenues of our research.

- ***Broader Implications***

Our research highlights the critical need for advanced cybersecurity mechanisms in the realm of digital image transmission over complex communication channels. Given the exponential growth of multimedia data transmission and the increased reliance on mobile communication systems, ensuring robust security has never been more pivotal.

- ***Challenges in Real-World Implementation***

While our proposed solution demonstrates promising results in a simulated environment, real-world challenges, such as hardware limitations, varying noise levels, and diverse channel conditions, can influence the performance. Addressing these challenges would require adaptive algorithms and hardware-software co-designs for optimal results.

- ***Scalability and Adaptability***

The proposed hybrid cybersecurity algorithm is designed to be both scalable and adaptable. Its modular structure allows for integration with other communication standards, making it a potential candidate for broader applications beyond SC-FDMA systems.

- ***Future Research Directions***

Building upon the foundations laid in this paper, future research could explore the integration of quantum-resistant algorithms, delve deeper into lightweight cryptographic solutions suitable for resource-constrained devices, and investigate the potential of applying deep learning techniques for enhanced watermarking and encryption processes. Another intriguing direction would be to evaluate the performance of our proposed solution under different types of adversarial attacks, ensuring its robustness against sophisticated cyber threats.

Furthermore, the overall comparison between schemes has been conducted in terms of PSNR, BER, and C_r metrics. The comparative study demonstrates that:

- For Pedestrian A channel, the DWT-LFDMA is the best of all studied cases as it reaches a BER of zero and a PSNR value approaching infinity at the smallest value of SNR of 12 dB compared to the other studied cases. It is also observed that the localized subcarrier mapping scheme has better performance than the interleaved subcarrier mapping scheme.
- For the Vehicular A channel, the DCT-LFDMA is the best of all studied cases as it reaches a BER of zero at the smallest value of SNR of 15 dB and a PSNR value approaching infinity at the smallest value of SNR of 18 dB compared to the other cases.
- The outcomes from the experiments reveal high-quality imperceptibility of the received decrypted watermarked images at SNR values of 12, and 18 dB, when Pedestrian A and Vehicular A channels are considered, respectively, which are sufficiently good values.
- The outcomes of the experiments also reveal the high correlation between the extracted watermark image at the receiver side and the original watermark image as it gives high correlation values at SNR values of 12, and 18 dB, over Pedestrian A and Vehicular A channels, which signifies high robustness.
- The histograms of the received encrypted and decrypted watermarked images show that the received encrypted watermarked images still maintain their uniform nature, and this makes the schemes stronger against different attacks. It is also evident that decrypted (retrieved) watermarked images are similar to the original ones. This means that the histogram gives a clear significance that the decryption has produced the original image.
- The histograms of extracted watermark images at the receiver side reveal that the extracted watermark images are highly correlated with the original watermark images. This means that the watermark has been extracted significantly at the receiver side.

- ***Basis for Conclusions on DWT-SC-FDMA and DCT-SC-FDMA Suitability***
- ***DWT-SC-FDMA in Pedestrian A Channels:***

The suitability of DWT-SC-FDMA for the transmission of digital images over Pedestrian A channels emerged from the following observations:

1. **Resilience to Multi-Path Propagation:** Pedestrian A channels often exhibit time dispersion due to multi-path propagation. DWT inherently provides multi-resolution analysis, which allows

better representation of signal in such environments. In our simulations, this translated to a higher PSNR for transmitted images, indicating better image quality.
2. **Lower Latency:** The decomposition nature of DWT resulted in reduced computational complexity, especially in dense urban pedestrian scenarios. This allowed for faster image transmission and decoding.

- ***DCT-SC-FDMA in Vehicular A Channels:***

Our choice of DCT-SC-FDMA for vehicular A channels was based on:

1. **Handling Doppler Shifts:** Vehicular A channels introduce higher Doppler shifts due to rapid mobility. DCT capability to represent signals in the frequency domain ensured that such shifts had minimal impact on the transmitted images. This was evident from the reduced BER in our simulation results for vehicular scenarios.
2. **Robustness to Noise:** DCT energy compaction property ensured that the image essential features were maintained in fewer coefficients. This proved beneficial in vehicular environments, where noise is more erratic. The transmitted images, when subjected to DCT-SC-FDMA, had fewer visible artifacts compared to other variants.

In summary, the selection of DWT-SC-FDMA for Pedestrian A channels and DCT-SC-FDMA for Vehicular A channels was driven by a combination of theoretical underpinnings of these transforms and the empirical results from our extensive simulations.

- ***Scope and Limitations:***
- ***Scope:***

This study primarily focuses on:

1. Analyzing the secure transmission of digital images over the SC-FDMA wireless communication system.
2. Investigating the effectiveness of the DCT-SVD watermarking technique combined with chaos and DNA-based image encryption.
3. Evaluating the performance of different SC-FDMA variants, particularly FFT-SC-FDMA, DCT-SC-FDMA, and DWT-SC-FDMA, in the context of Pedestrian A and Vehicular A channel models using QAM.

- ***Limitations:***

1. **Encryption Techniques:** While we implemented encryption based on chaos and DNA encoding, other contemporary encryption methods were not explored.
2. **Channel Models:** This research is confined to Pedestrian A and Vehicular A channel models. Other potential channel models may yield different results.
3. **Watermarking:** The watermarking technique was centered on DCT-SVD. Alternative watermarking strategies might present varying efficacy levels in image security.
4. **Modulation:** The study employed QAM. Other modulation schemes could affect the system performance and were not part of this research.

By highlighting these areas, we aim to guide readers in understanding the specific focus of our research and the areas where caution should be exercised when generalizing our findings. Future work can address these limitations, broadening the research spectrum in the domain of digital image transmission over wireless communication channels.

7 Conclusion and Future Work

Efficient, reliable, and secure means of wireless communication for the transfer of digital data (text, images, audio, and video) from source to destination is becoming a prime requirement in present-day wireless communications. This paper considered the development of different schemes for encrypted watermarked image transmission over a wireless SC-FDMA system and the analysis of their performances through simulations. The image transmission from one place to another using wireless communication systems requires more security. The study presented two security stages for image transmission over the wireless SC-FDMA system. The first stage is the watermarking. The watermark image shows itself in the cover image with the proposed hybrid DCT-SVD algorithm. As a result, it gives birth to a robust watermarked image. The second stage is to encrypt the watermarked image using the image encryption algorithm based on chaos and DNA encoding introduced earlier in this study. The encrypted watermarked image is then transmitted on a wireless SC-FDMA system. Three different schemes have been considered: FFT-based SC-FDMA, DCT-based SC-FDMA, and DWT-based SC-FDMA. Each scheme is simulated considering either localized or interleaved subcarrier mapping and MMSE equalizer. This study depends on two wireless channel models, Pedestrian A and Vehicular A. The foundational concepts in this paper provide several potential avenues for future exploration and development:

- Integration with Other Communication Standards: While our study primarily focused on the SC-FDMA system, it would be intriguing to test and adapt our hybrid cybersecurity algorithm for other emerging communication standards. It would ascertain the versatility and scalability of our proposed solutions.
- Enhancing Encryption Techniques: The current implementation depends on chaos and DNA encoding for image encryption. Exploring the fusion of quantum encryption methods or leveraging advanced cryptographic techniques could further strengthen the security facet of our framework.
- Advanced Watermarking Methods: Although the DCT-SVD watermarking technique showed promising results, integrating deep-learning-based watermarking could provide more robustness against sophisticated watermark removal or tampering attacks.
- Real-world Testing and Deployment: Conducting real-world experiments beyond simulations, especially in diverse environmental conditions and variable hardware configurations, would validate the practical applicability and robustness of our algorithm.
- Optimization for Real-time Transmission: Considering the ever-growing demand for real-time multimedia communications, optimizing the proposed algorithm for lower latency without compromising security would be a significant advancement.

We anticipate that pursuing these future research directions will significantly enhance the impact and applicability of our work in the broader domain of secure digital image transmission.

Acknowledgement: This work is funded by the Deanship of Scientific Research, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors are very grateful to all the institutions in the affiliation list for successfully performing this research work. The authors would like to thank Prince Sultan University for their support.

Funding Statement: This research project was funded by the Deanship of Scientific Research, Princess Nourah bint Abdulrahman University, through the Program of Research Project Funding After Publication, Grant No. (44-PRFA-P-131).

Author Contributions: Study conception and design: Naglaa F. Soliman, Fatma S. Fadl, Walid El-Shafai; data collection: Naglaa F. Soliman, Maali Alabdulhafith and Fathi E. Abd El-Samie; analysis and interpretation of results: Naglaa F. Soliman, Walid El-Shafai, Mahmoud I. Aly, Maali Alabdulhafith; draft manuscript preparation: Naglaa F. Soliman, Walid El-Shafai, Mahmoud I. Aly. supervision and funding acquisition: Naglaa F. Soliman, Walid El-Shafai. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data will be available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare that hey have no conflicts of interest to report regarding the present study.

References

[1] A. Alarifi, S. Sankar, T. Altameem, K. C. Jithin, M. Amoon and W. El-Shafai, "A novel hybrid cryptosystem for secure streaming of high efficiency H.265 compressed videos in IoT multimedia applications," *IEEE Access*, vol. 8, pp. 128548–128573, 2020. doi: 10.1109/ACCESS.2020.3008644.

[2] F. Ikbal and R. Gopikakumari, "Image block generation from block-based SMRT in colour image encryption and its performance analysis," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8459–8477, 2022. doi: 10.1016/j.jksuci.2021.08.026.

[3] J. Xin, H. Hu, and J. Zheng, "3D variable-structure chaotic system and its application in color image encryption with new Rubik's cube-like permutation," *Nonlinear Dynam.*, vol. 111, no. 8, pp. 7859–7882, 2023. doi: 10.1007/s11071-023-08230-2.

[4] K. Alhumyani, "Dual image cryptosystem using henon map and discrete fourier transform," *Intell. Autom. Soft Comput.*, vol. 36, no. 3, pp. 1–13, 2023. doi: 10.32604/iasc.2023.034689.

[5] M. Hassan, S. Zaman, S. Mollick, M. Hassan, and M. Raihan, "An efficient Apriori algorithm for frequent pattern in human intoxication data," *Innov. Syst. Software Eng.*, vol. 19, no. 1, pp. 61–69, 2023. doi: 10.1007/s11334-022-00523-w.

[6] A. Bahaddad, K. Almarhabi, and S. Abdel-Khalek, "Image steganography technique based on bald eagle search optimal pixel selection with chaotic encryption," *Alexandria Eng. J.*, vol. 7, no. 5, pp. 41–54, 2023. doi: 10.1016/j.aej.2023.05.051.

[7] S. Bhowmik and S. Acharyya, "Image encryption approach using improved chaotic system incorporated with differential evolution and genetic algorithm," *J. Inf. Secur. Appl.*, vol. 7, no. 2, pp. 103–119, 2023. doi: 10.1016/j.jisa.2022.103391.

[8] O. Faragallah *et al.*, "Secure color image cryptosystem based on chaotic logistic in the FrFT domain," *Multimed. Tools Appl.*, vol. 79, no. 3, pp. 2495–2519, 2020. doi: 10.1007/s11042-019-08190-z.

[9] M. Eichelberg, K. Kleber, and M. Kämmerer, "Cybersecurity in PACS and medical imaging: An overview," *J. Digit. Imaging*, vol. 33, no. 6, pp. 1527–1542, 2020. doi: 10.1007/s10278-020-00393-3.

[10] M. Eichelberg, K. Kleber, and M. Kämmerer, "Cybersecurity challenges for PACS and medical imaging," *Acad. Radiol.*, vol. 27, no. 8, pp. 1126–1139, 2020. doi: 10.1016/j.acra.2020.03.026.

[11] M. Hassan, S. Mollick, and F. Yasmin, "An unsupervised cluster-based feature grouping model for early diabetes detection," *Healthcare Anal.*, vol. 2, no. 6, pp. 100–112, 2022.

[12] W. El-Shafai, "Pixel-level matching based multi-hypothesis error concealment modes for wireless 3D H.264/MVC communication," *3D Res.*, vol. 6, no. 3, pp. 1–11, 2015. doi: 10.1007/s13319-015-0064-5.

[13] M. Hassan, A. Karim, S. Mollick, S. Azam, A. Al Haque and Al Haque, "An apriori algorithm-based association rule analysis to detect human suicidal behaviour," *Procedia Comput. Sci.*, vol. 21, no. 9, pp. 1279–1288, 2023. doi: 10.1016/j.procs.2023.01.412.

[14] M. Hassan and S. Mollick, "Efficient prediction of water quality index (WQI) using machine learning algorithms," *Human-Centric Intell. Syst.*, vol. 1, no. 3, pp. 1–14, 2021. doi: 10.2991/hcis.k.211203.001.

[15] Z. Faheem, D. Hanif, and A. Baz, "An edge inspired image watermarking approach using compass edge detector and LSB in cybersecurity," *Comput. Electr. Eng.*, vol. 11, no. 1, pp. 108–131, 2023. doi: 10.1016/j.compeleceng.2023.108979.
[16] A. Sarker, A. Canto, M. Kermani, and R. Azarderakhsh, "Error detection architectures for hardware/software co-design approaches of number-theoretic transform," *IEEE Trans. Comput.-Aid. Des. Integr. Circ. Syst.*, vol. 91, no. 8, pp. 1023–1049, 2022. doi: 10.1109/TCAD.2022.3218614.
[17] S. Singh and G. Bhatnagar, "A new robust watermarking system in integer DCT domain," *J. Vis. Commun. Image Representation*, vol. 53, no. 5, pp. 86–101, 2018. doi: 10.1016/j.jvcir.2018.03.006.
[18] M. Kermani, R. Azarderakhsh, and J. Xie, "Error detection reliable architectures of Camellia block cipher applicable to different variants of its substitution boxes," *Int. J. Inf. Technol. Secur.*, vol. 11, no. 4, pp. 107–119, 2016. doi: 10.1109/AsianHOST.2016.7835560.
[19] J. X. Chen, Y. Zhang, J. C. Li, and L. B. Zhang, "Security enhancement of double random phase encoding using rear-mounted phase masking," *Opt. Laser. Eng.*, vol. 101, no. 2, pp. 51–59, 2018. doi: 10.1016/j.optlaseng.2017.09.019.
[20] K. Prabha and I. Sam, "A novel blind color image watermarking based on walsh hadamard transform," *Multimed. Tools Appl.*, vol. 79, no. 5, pp. 6845–6869, 2020. doi: 10.1007/s11042-019-08212-w.
[21] H. Zhang, C. Wang, and X. Zhou, "A robust image watermarking scheme based on SVD in the spatial domain," *Future Internet*, vol. 9, no. 45, pp. 201–211, 2017. doi: 10.3390/fi9030045.
[22] T. Takore, P. Kumar, and G. Devi, "A new robust and imperceptible image watermarking scheme based on hybrid transform and PSO," *Int. J. Security Syst. Appl.*, vol. 11, no. 4, pp. 50–63, 2018. doi: 10.5815/ijisa.2018.11.06.
[23] J. Liu and X. He, "A review study on digital watermarking," in *Proc. 1st Int. Conf. Inf. Commun. Technol., ICICT*, Karachi, Pakistan, 2005, pp. 337–341.
[24] R. Olanrewaju, "Development of intelligent digital watermarking via safe region," Ph.D. Thesis, Kulliyyah of Engineering, International Islamic Univ. Malaysia, Selangor, Malaysia, 2011.
[25] U. Yadav, J. Sharma, D. Sharma, and P. Sharma, "Different watermarking techniques & its applications: A review," *Int. J. Sci. Eng. Res.*, vol. 5, no. 4, pp. 1288–1294, 2014.
[26] N. Cvejic, "Algorithms for audio watermarking and steganography," Master's Thesis, Dept. of Electrical and Information Engineering, Univ. of Oulu, Oulu, Finland, 2004.
[27] J. Sang and M. Alam, "Fragility and robustness of binary-phase-only-filter-based fragile/semi fragile digital image watermarking," *IEEE Trans. Instrum. Meas.*, vol. 57, no. 3, pp. 595–606, 2008. doi: 10.1109/TIM.2007.911585.
[28] W. El-Shafai, F. Mohamed, H. Elkamchouchi, M. Abd-Elnaby, and A. ElShafee, "Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm," *IEEE Access*, vol. 9, pp. 1–25, 2021. doi: 10.1109/ACCESS.2021.3082940.
[29] X. Wang and C. Chang, "Reversal of pixel rotation: A reversible data hiding system towards cybersecurity in encrypted images," *J. Vis. Commun. Image Represent.*, vol. 8, no. 2, pp. 103–120, 2022. doi: 10.1016/j.jvcir.2021.103421.
[30] O. Faragallah, E. El-Rabaie, M. El-Halawany, and F. A. El-Samie, "Efficient multi-level security for robust 3D color-plus-depth HEVC," *Multimed. Tools Appl.*, vol. 77, no. 23, pp. 30911–30937, 2018. doi: 10.1007/s11042-018-6036-z.
[31] S. Katti, V. Namuduri, and K. Namuduri, "A practical approach for evaluating the capacity of watermarking channel," in *Proc. Int. Conf. Intell. Sens. Inf. Process.*, Chennai, India, 2005, pp. 193–198.
[32] J. Smith and D. Watson, "Advancements in digital image encryption using chaos theory," *J. Cybersecur. Digit. Commun.*, vol. 9, pp. 35004–35026, 2023.
[33] H. Lee and M. Kim, "Performance metrics for SC-FDMA systems in modern wireless communication," *IEEE Trans. Wirel. Commun.*, vol. 5, no. 4, pp. 1288–1294, 2022.
[34] L. Martin and T. Rogers, "Exploring DNA-based image encryption techniques for secure transmission," *J. Adv. Image Process.*, vol. 79, no. 5, pp. 6845–6869, 2020.

[35] P. Gupta and R. Singh, "An analysis of DCT-SVD watermarking in the era of broadband communication," *J. Multimed. Syst. Appl.*, vol. 101, no. 2, pp. 51–59, 2022.
[36] G. Alvarez and M. Lopez, "SC-FDMA: A review of recent developments and future trends," *IEEE Wirel. Commun. Mag.*, vol. 9, no. 45, pp. 201–211, 2022.
[37] Y. Chan and L. Wong, "Comparative study of FFT, DCT, and DWT in SC-FDMA image transmission systems," *J. Commun. Syst.*, vol. 11, no. 4, pp. 50–63, 2018, 2023.