Cryptographic Techniques in Digital Media Security: Current Practices and Future Directions

Gongling ZHANG
Luoyang Cultural Tourism Vocational College, Luoyang 471000, China

***Abstract*—Content privacy and unauthorized access to copyrighted digital media content are common in the dynamic, fast-paced digitalized media marketplace. Cryptographic methods are the foundation of modern digital media security, and they must ensure the security, integrity, and authenticity of digital media data. This article analyses cryptographic methods that are used to protect digital media content. The paper reviews the main cryptographic concepts, such as symmetric cryptography, asymmetric cryptography, hash functions, and digital signatures. The paper also discusses some popular approaches: encryption, Digital Rights Management (DRM), watermarking, and solutions based on blockchain. Finally, we highlight implementation challenges such as key management and scalability and identify emerging trends such as quantum-safe cryptography and privacy-preserving techniques. By presenting the current research results and discussing the directions for the future, the study aims to pave the way for secure, efficient, and robust cryptographic solutions for digital media protection, leading to sustainable development, innovation, and secure communication of digital content among users.**

***Keywords*—Digital media; cryptographic; content security; digital rights management; watermarking, blockchain**

I. INTRODUCTION

Digital content is now more dominant than tangible media in terms of dissemination and usage [1]. Inherent properties such as the ability to reproduce identical documents easily and disseminate them over the Internet through wired and wireless communication have relevant ramifications for intellectual property rights [2]. Thus, the sharing of the content generally takes place beyond the limits of copyright law [3]. Digital products have the potential to be copied, replicated, and distributed across the globe within minutes of issuance, making detection and enforcement very difficult [4]. The illegal redistribution and exploitation of intellectual information may result in substantial financial losses for content producers and owners, with industry estimates suggesting that these losses amount to billions of dollars each year [5].

Social media platforms facilitating global communication and information dissemination have become breeding grounds for image sharing [6]. With billions of images uploaded daily, concerns about illegal access, manipulation, and unauthorized distribution are growing. Applying digital image watermarks is emerging as a promising technique to address these security challenges [7]. However, effective watermarking depends on three crucial requirements: imperceptibility, robustness, and embedding capacity. The watermarked image should be visually indistinguishable from the original image so as not to impact the user experience [8]. The watermark should resist attacks such as compression, noise, or cropping to ensure its durability and accuracy and protect copyright. The watermark should embed sufficient information to reliably identify the owner or copyright holder. These requirements often have trade-offs. For example, spatial domain watermarking techniques provide high embedding capacity and imperceptibility but are not robust to manipulation. Conversely, spectral domain techniques achieve higher robustness but may result in visible artifacts that impact imperceptibility.

To achieve an optimal balance between these competing demands, researchers have explored hybrid approaches that leverage both spatial and spectral domains. Nature-inspired metaheuristic optimization algorithms were employed to optimize the embedding strength of the watermark, aiming to find a balance between imperceptibility, robustness, and embedding capacity [9, 10]. However, developing effective fitness functions that balance exploration (searching for novel solutions) and exploitation (refining promising solutions) remains an ongoing challenge.

Digital transformation, driven by the Internet of Things (IoT) and the increasing demand for secure and real-time communication, fundamentally changes how we interact with information and the world around us [11]. IoT envisions a future in which nearly every object is connected to the Internet and generates and transmits massive amounts of data, including personal, sensitive, and confidential information [12]. While these advances offer unprecedented opportunities, they pose significant security challenges. Smart cities and advances like cryptocurrencies hold enormous potential to reshape the coming decade, but the inherent vulnerabilities of these technologies raise concerns about privacy and communications security [13].

The purpose of this article is to discuss the principles of cryptographic technologies that can be used to prevent unauthorized access to digital media content and its piracy. The article begins with an introduction to the importance of digital media security and the function of cryptography. Basic cryptographic principles of symmetric and asymmetric encryption, as well as hash functions and digital signatures, are examined. Various security strategies are then discussed, including encryption, Digital Rights Management (DRM), watermarking, and blockchain security solutions. The discussion also addresses the difficulties and disadvantages of applying these approaches, new trends and promoting possible developments. Finally, the paper offers a brief conclusion with key findings and suggestions for where further research should be conducted.

II. BACKGROUNDS

Information security protects data from unauthorized access, theft, alteration, or destruction. This covers various information formats, including text, images, audio, and video [14]. Two main approaches are used to ensure information security: cryptography and steganography. Cryptography uses complex mathematical algorithms to encrypt or scramble data into an unreadable format (ciphertext). This makes the data unreadable even if unauthorized persons intercept it. However, encryption itself can sometimes signal valuable information. To counteract this limitation, steganography hides communication itself. Steganography embeds confidential messages in a seemingly innocuous cover object, such as an image or audio file. This allows data to be passed on unnoticed by eavesdroppers. Even if the cloak is intercepted, the information remains hidden, providing an additional layer of security. Fig. 1 illustrates the general process of digital media content encryption. A variety of multimedia encryption applications are also illustrated in Fig. 2.

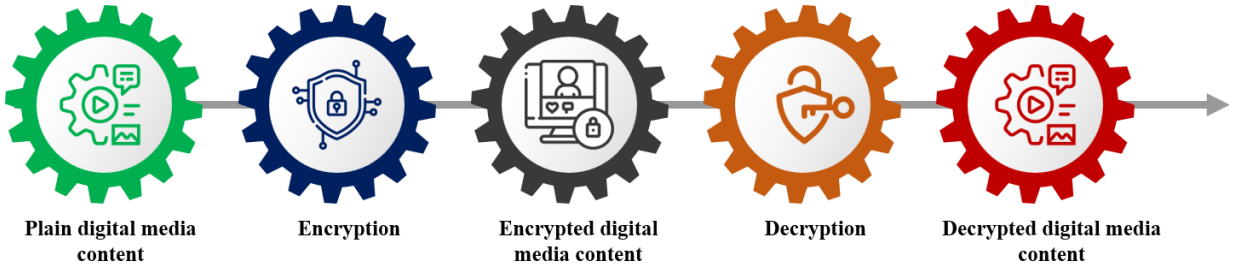

Fig. 1. General process of digital media content encryption.

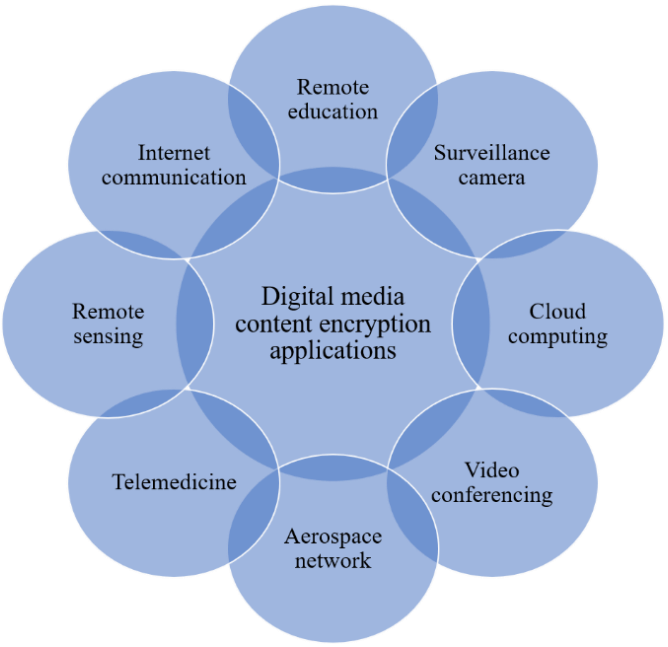

Fig. 2. Applications of multimedia encryption in various domains.

A. Symmetric Cryptography

This is also called secret-key cryptography, where the same secret key is used for encryption and decryption. This key should be kept secret by both the sender and the receiver to enhance the security of the passed information. The basis for the use of symmetric cryptography is the secrecy of the key and the choice of the algorithm used to encrypt the data. Symmetric encryption algorithms are generally classified into block ciphers and stream ciphers [15]. Block ciphers, like the Advanced Encryption Standard (AES), process data in fixed-size blocks during encryption. In contrast, stream ciphers, such as Rivest Cipher 4 (RC4), encrypt data one bit or byte at a time. The selection between block and stream ciphers depends on the application's requirements, such as prioritizing high-speed encryption or resistance to specific attack types. Symmetric cryptography underpins the security of various digital media content due to its efficiency and speed. A comparison of common symmetric encryption algorithms is presented in Table I.

- Content encryption: To prevent unauthorized access, digital media files (videos, audio, images) are often encrypted using symmetric algorithms. Content providers can ensure that only authorized users with the corresponding decryption key can access the media. For instance, streaming services like Netflix and Spotify might leverage the Advanced Encryption Standard (AES) to protect their media files during transmission and storage.

- DRM: Symmetric cryptography is critical in enforcing DRM systems' access controls and usage policies. The media content is encrypted with a symmetric key securely distributed only to authorized users. The DRM system manages key distribution and revocation, guaranteeing that content decryption and access are restricted to legitimate users.
- Secure streaming: Real-time encryption of media content before transmission is essential for live streaming scenarios. Due to their ability to encrypt data on the fly, stream ciphers are particularly well-suited for this purpose. Encrypted streams are transmitted over networks, ensuring intercepted data remains unintelligible without the decryption key.
- Storage encryption: Symmetric encryption safeguards digital media stored on servers or user devices. By encrypting media files at rest, service providers can prevent unauthorized access in the event of a data breach or physical theft of storage devices.

TABLE I. SYMMETRIC CRYPTOGRAPHY

Algorithm	Type	Key size (bits)	Block size (bits)	Example use cases
AES	Block cipher	128, 192, 256	128	Secure file transfer and encryption of sensitive data
DES	Block cipher	56	64	Legacy systems, previously used in banking transactions
RC4	Stream cipher	40-2048	Variable	Secure network protocols (e.g., WEP, SSL/TLS)
3DES	Block cipher	112, 168	64	Financial services and legacy systems requiring higher security

B. Asymmetric Cryptography

Asymmetric cryptography, also known as public-key cryptography, utilizes a mathematically elegant solution for secure communication by employing two distinct keys for encryption and decryption: a public key and a private key [16]. Unlike symmetric cryptography, the public key is openly distributed, allowing anyone to encrypt data intended for a specific recipient. The private key, conversely, is meticulously guarded by its owner and serves as the sole means to decrypt the data. This clear separation of keys addresses a fundamental challenge in symmetric cryptography: secure key distribution. Public-key cryptographic systems are built upon mathematical problems that are difficult to solve practically without possessing the corresponding private key. Well-established algorithms in this domain include RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), and DSA (Digital Signature Algorithm). These algorithms mathematically guarantee that data encrypted with a public key can only be decrypted by the holder of the corresponding private key, offering a secure method for exchanging information even over untrusted channels. Asymmetric cryptography is critical in securing digital media content, and enhancing security and user trust. It provides several key advantages over symmetric cryptography, particularly in areas where secure key distribution and verification of content authenticity are paramount. Table II presents a comparison of common asymmetric encryption algorithms.

TABLE II. ASYMMETRIC CRYPTOGRAPHY

Algorithm	Key type	Key size (bits)	Security level	Example use cases
RSA	Public/private	1024, 2048, 4096	High	Secure email, digital signatures, and SSL/TLS
ECC	Public/private	160-521	Very high	Mobile devices, digital signatures, and secure communications
DSA	Public/private	1024-3072	High	Digital signatures and secure document verification
ElGamal	Public/private	256-4096	High	Encrypted key exchange and digital signatures

- Secure key exchange: A primary application is a secure key exchange for symmetric encryption. Even if attackers intercept communication channels, the asymmetric system ensures the confidentiality of symmetric keys to encrypt media content. For instance, streaming services might leverage asymmetric cryptography to exchange encryption keys securely during the initial connection setup.
- Digital signatures and content authentication: Digital signatures, created using asymmetric cryptography, verify the authenticity and integrity of digital media. When content creators sign a media file with their private key, anyone can verify the signature using the corresponding public key. This ensures the content originates from the claimed source and has not been tampered with. This mechanism is widely used in software distribution and updates to guarantee the authenticity of digital media.
- Certificate-based authentication and secure communication: Digital certificates issued by trusted authorities rely on asymmetric cryptography to authenticate digital media distribution and consumption entities. These certificates ensure users connect to legitimate services and that media providers distribute content securely. For example, HTTPS protocols use certificates to secure communication between web browsers and streaming services.
- Enhanced DRM: Asymmetric cryptography strengthens DRM systems by facilitating secure key management and distribution. Public-key cryptography can encrypt content keys and distribute them only to authorized devices. These devices then use their private keys to decrypt the content keys and access the media. This restricts access to licensed users and devices, preventing unauthorized distribution and piracy.
- Secure content delivery with Content Distribution Networks (CDNs): CDNs leverage asymmetric cryptography to secure digital media distribution across

multiple servers. By encrypting media files with public keys and using private keys for decryption at endpoint servers, CDNs safeguard the integrity and confidentiality of media during transit, mitigating the risk of interception or tampering.

C. Hash Functions

Hash functions are cryptographic primitives that map arbitrary-length inputs to fixed-length outputs, typically represented as hexadecimal strings. These output values, or hash codes or values, possess the crucial uniqueness property. The corresponding hash value will be unique for any given input, and even minor alterations will result in a significantly dissimilar hash value. This phenomenon is known as the avalanche effect. Additionally, hash functions are deterministic, ensuring that identical inputs consistently produce the same hash value. Table III provides a comparison of common cryptographic hash functions.

TABLE III. HASH FUNCTIONS

Algorithm	Output size (bits)	Security level	Use cases
MD5	128	Insecure	Legacy systems and checksum verification
SHA-1	160	Insecure	Legacy systems and integrity checks
SHA-256	256	Secure	Digital signatures and integrity verification
SHA-512	512	Very secure	High-security applications and blockchain

A confluence of critical properties characterizes effective cryptographic hash functions. Determinism guarantees that identical inputs invariably produce the same hash value. Additionally, computation efficiency is paramount for real-world applications. Two fundamental properties ensure the robustness of hash functions against cryptographic attacks. Preimage resistance makes it computationally infeasible to retrieve the original input solely from the hash value. Collision resistance, on the other hand, safeguards against the possibility of finding two distinct inputs that generate the same hash output.

Furthermore, hash functions generate fixed-length outputs irrespective of the input size, enhancing their efficiency and facilitating comparisons. Common cryptographic hash functions include MD5 (though currently considered insecure) and SHA-1 (deprecated). The SHA-2 family, encompassing algorithms like SHA-256 and SHA-512, is now the recommended standard for secure hashing. Hash functions serve as a cornerstone for guaranteeing the integrity of digital media content. They provide a mechanism to verify that data remains unaltered or uncorrupted during transmission, storage, or manipulation.

- Data integrity verification: Hash functions safeguard digital media's integrity during transfers or storage across networks and diverse locations. By computing a hash value (unique digital fingerprint) for the original content, subsequent comparisons with the hash of the received or stored file can expose any modifications. This approach is essential for upholding trust in digital media distribution channels, cloud storage solutions, and content delivery networks.
- Digital signatures and certificates: Hash functions are instrumental in creating digital signatures, a cornerstone of digital media security. When a digital signature is generated, the hash of the content is encrypted with the sender's private key. This encrypted hash, often called a digital signature, is transmitted with the media. The recipient can decrypt the signed hash using the sender's public key and compare it to the hash value computed from the received content. If the hash values match, it confirms the content's integrity and authenticity, signifying that it remains unaltered since the signature was created.
- Content verification in blockchain: Blockchain technology, with its potential for secure digital media management, leverages hash functions to verify the integrity of content stored on the blockchain. Each block within a blockchain incorporates a hash value referencing the preceding block, effectively creating an immutable chain of records [17]. This immutability ensures that any attempt to tamper with a single piece of content would necessitate altering all subsequent blocks, rendering such efforts highly impractical.
- Deduplication and data management: Hash functions are valuable in identifying duplicate files within extensive digital media libraries. Systems can efficiently detect and manage duplicate content by generating and comparing hash values for various files. This optimization translates to improved storage utilization and streamlined retrieval processes.
- Integrity checks in DRM systems: DRM systems rely on hash functions to safeguard the integrity of protected media content. Verifying that the content has not been tampered with is crucial for maintaining the integrity of protected materials and ensuring compliance with licensing agreements.

D. Digital Signatures

Digital signatures are cryptographic mechanisms underpinning the verification of authenticity and integrity in digital messages and documents. Analogous in function to handwritten signatures, they offer a significantly enhanced level of security. The process of creating a digital signature leverages public-key cryptography. A unique signature is generated by encrypting a cryptographic hash of the message or document with the sender's private key. This signature can be validated by anyone possessing the corresponding public key, assuring that the document has not been tampered with and confirming the sender's identity. Common digital signature algorithms are listed in Table IV.

Digital signatures offer crucial properties: authentication, integrity, and non-repudiation. Authentication verifies the sender's identity, guaranteeing that the message or document originates from a legitimate source. Integrity, achieved through hash functions, ensures that the content has not been altered during transmission. Any modification to the content will result in a failed verification process due to a mismatch between the

calculated hash and the one embedded within the signature. Finally, non-repudiation prevents the sender from denying having sent a digitally signed document, thereby establishing legal validity and accountability. Digital signatures are a cornerstone for securing digital media content across various distribution and access channels. Their ability to verify authenticity and integrity fosters trust and combats potential security threats.

TABLE IV. DIGITAL SIGNATURES

Algorithm	Key type	Key size (bits)	Security level	Example use cases
RSA	Public/private	1024, 2048, 4096	High	Document signing and software distribution
ECDSA	Public/private	160-521	Very high	Secure transactions and blockchain
DSA	Public/private	1024-3072	High	Secure communications and legal document verification
EdDSA	Public/private	256-512	Very high	Secure messaging and financial transactions

- Content distribution verification: When digital media like music, videos, or e-books are distributed online, digital signatures safeguard their authenticity. Content creators or distributors can cryptographically sign their media files. Users can then verify these signatures using the publicly available content creator key. This process ensures the content hasn't been tampered with or corrupted during distribution, protecting users from unknowingly acquiring compromised media.
- Software and firmware updates: Digital signatures are critical in software and firmware updates for digital media devices like streaming boxes, smart TVs, and gaming consoles. Manufacturers sign update files with their private keys. Devices verify these signatures before installing the updates, guaranteeing that only legitimate and unaltered updates are applied. This mitigates the risk of installing malicious software disguised as updates.
- Blockchain and content authentication: With its potential for secure digital media management, Blockchain technology utilizes digital signatures for transaction authentication and ownership verification of digital assets. The content owner signs every transaction involving digital media content, and these signatures are recorded on the blockchain. This creates a transparent and tamper-proof record of ownership and distribution history.
- Secure online transactions: In e-commerce platforms selling digital media like music, videos, and software, digital signatures guarantee the authenticity of the purchased content. Customers can verify that the digital products they receive are genuine and unaltered. This enhances trust and transparency in the transaction process for consumers and vendors.
- Copyright protection and legal evidence: Digital signatures offer legal proof of ownership and authenticity, which is crucial for copyright protection and legal disputes. Content creators can leverage digital signatures to establish their rights over their creations. These signatures can then be presented as evidence in court cases related to copyright infringement.

III. REVIEW OF APPROACHES

The widespread adoption of image formats, especially JPEG, has opened avenues for embedding additional information within these files. While stenographic techniques utilizing the least significant bits have been dominant, this research proposes alternative methods. Harran, et al. [18] demonstrated the feasibility of incorporating a digital certificate alongside its corresponding metadata directly into an image file. This metadata references the issuing entity responsible for the certificate. Despite variations across devices, operating systems, and applications, JPEG files exhibit remarkable structural consistency. The proposed approach strategically inserts references to the issuing company within the file's metadata. This integration offers a distinct advantage: the digital certificate remains tethered to the file it applies to, ensuring it travels together throughout the file's lifecycle. The research ultimately establishes the potential of file metadata to house additional data that bolsters the integrity, authenticity, and provenance of the digital content embedded within the file. This approach paves the way for innovative methods to secure and verify digital content using existing file structures.

Table V summarizes the proposed approaches for embedding and securing digital media, highlighting key techniques, advantages, and use cases. Gurunathan and Rajagopalan [19] proposed a steganographic technique for embedding secret messages within a cover image using LSB substitution to evade detection by potential interceptors. This work builds upon the core concept of LSB substitution but introduces modifications to improve image quality and message capacity while maintaining security. Inspired by existing approaches that divide cover images into blocks, the proposed method partitions the cover image and the secret message into equal-sized blocks (typically 8x8 pixels). This strategy aims to achieve a balance between embedding capacity and image quality. A key innovation lies in utilizing the Cuckoo Search (CS) algorithm. Unlike prior methods that employ a single substitution matrix for the entire image, the proposed approach leverages CS to find an optimal substitution matrix for each block. This approach aims to achieve a more nuanced embedding process, optimizing message concealment within each block while minimizing visual artifacts in the resulting stego-image (the image containing the hidden message). The final stage involves evaluating the quality of the stego-image, the message capacity, and the security level of the proposed method. These metrics are then compared to existing techniques based on the Joint Photographic Experts Group (JPEG) standard and Joint Quantization Table Modification (JQTM). Experimental results, as reported by the authors, demonstrate that the proposed method surpasses both JPEG and JQTM-based methods in terms of image quality, security level, and message embedding capacity.

TABLE V. PROPOSED APPROACHES FOR EMBEDDING AND SECURING DIGITAL MEDIA

Authors	Approach	Key techniques	Advantages
Harran, et al. [18]	Embedding digital certificates in JPEG files	Metadata embedding	Ensures certificate travels with the file, enhances integrity and authenticity
Gurunathan and Rajagopalan [19]	Steganography using LSB substitution with Cuckoo Search algorithm	LSB substitution, Cuckoo Search	Improves image quality and message capacity, optimizes message concealment
Gafsi, et al. [20]	Hybrid image encryption using asymmetric and symmetric cryptography	RSA, AES-256, SHA-2	High security, robust against cryptanalysis attacks
Panchal, et al. [22]	Document security using fingerprint biometrics	Biometric feature extraction, convolution coding	High true positive rate, no need to store encryption keys
William, et al. [21]	Hybrid cryptographic solution merging AES, ECC, and SHA-256	AES, ECC, SHA-256	Enhanced efficiency for text encryption, secure data integrity
Yasser, et al. [23]	Multimedia encryption using chaotic dynamics and 2D alteration models	Chaotic maps, hybrid chaotification	Strong key sensitivity, high resistance to attacks
Sanivarapu, et al. [24]	Image watermarking scheme using cryptographic techniques and QR code scrambling	QR code, DWT, SVD, chaotic logistic map	Resilient to image processing attacks, maintains minimal visual distortion
Alarifi, et al. [25]	Hybrid cryptosystem for securing HEVC video streams	DNA sequences, Arnold chaotic map, Mandelbrot sets	Robust and enhanced security for HEVC video streaming

Gafsi, et al. [20] presented a novel image encryption system designed to achieve high security for digital images. Their approach leverages a combination of asymmetric and symmetric cryptography to provide robust protection. The asymmetric component utilizes the well-established RSA algorithm. RSA employs a public key for encryption and a private key for decryption, ensuring secure key distribution and management. However, image encryption relies on the AES-256 algorithm in Counter (CTR) mode. This combination offers a strong foundation for image data encryption. Furthermore, the system incorporates the SHA-2 hashing function. SHA-2 serves as a cryptographic hash function, generating a unique fingerprint of the original image data. This fingerprint can be used for integrity verification, ensuring the image has not been tampered with during encryption or decryption. The effectiveness of the proposed system was evaluated using various established tools and tests commonly employed within the image cryptography community. These tests utilized a diverse set of standard, non-compressed images. The experimental and analytical results indicate that the encryption scheme offers robustness and resistance against known cryptanalysis attacks. These positive results suggest the proposed method achieves high performance and efficiency, making it suitable for applications requiring strong image protection in various domains, such as military communication and securing sensitive data for personal privacy.

William, et al. [21] proposed a novel cryptographic solution that merges three distinct cryptographic primitives: a symmetric algorithm (AES), an asymmetric algorithm (ECC), and a hash function (SHA-256). SHA-256 is a cryptographic hash function that generates a unique message digest from the input data. This digest is a fingerprint to verify data integrity and expose potential tampering attempts. The proposed hybrid approach resembles existing techniques that leverage AES for encrypting textual and graphical data. However, the authors posit that their solution offers enhanced efficiency, particularly text encryption, compared to prior methods. While acknowledging the current limitations in image encryption speed, they suggest that future advancements could optimize the solution for improved image encryption performance.

Panchal, et al. [22] proposed a novel document security mechanism that leverages fingerprint biometrics. This system extracts unique features from a user's fingerprint captured by a biometric sensor. These features are then processed using convolution coding principles to generate a unique code. This unique code is the foundation for creating cryptographic keys for encrypting and decrypting user documents. A rigorous evaluation of the proposed approach, involving experimentation with various standard fingerprint images within a database, yielded impressive results. The system achieved a high true positive rate of 95%, indicating accurate identification of authorized users.

Furthermore, the system yielded a 0% false negative rate, ensuring no instances where authorized users were mistakenly denied access. This system offers several significant advantages. Firstly, it generates a unique key for each user, eliminating the need to store a central template of biometric data, which can be a security vulnerability. Secondly, the system avoids storing any encryption keys, further enhancing security. Finally, the reported efficiency suggests the system is suitable for real-world applications due to its speed and accuracy. These qualities make it a promising solution for developing robust data storage security systems.

Yasser, et al. [23] introduce novel multimedia encryption schemes that leverage chaotic dynamics and 2D alteration models to achieve high-security data transmission. Their approach revolves around a new perturbation-based data encryption method applicable to confusion and diffusion rounds. The core novelty lies in the hybrid chaotification structure, which combines multiple chaotic maps for enhanced media encryption. These blended maps generate control parameters for the permutation (shuffling) and diffusion (substitution) stages within the encryption process. The proposed schemes maintain the high encryption quality characteristic of chaotic systems and boast additional advantages. These include strong key sensitivity, resistance to unauthorized key derivation, and low residual clarity, minimizing the potential for intelligible information leakage from the encrypted media. Extensive security and differential analyses demonstrate the efficacy of the proposed schemes for securing multimedia transmissions. The encrypted media exhibits a high degree of resistance against various attacks. Additionally, statistical evaluations using established metrics for specific media types reveal that the schemes achieve low

residual intelligibility while maintaining statistically sound properties in the recovered data.

Sanivarapu, et al. [24] introduced a novel image watermarking scheme that utilizes cryptographic techniques to ensure copyright protection and content authentication. Their method centers around a watermark image containing a public-key/private-key pair generated through a cryptosystem. This watermark is then encoded into a quick response (QR) code. The QR code is scrambled using a chaotic logistic map to enhance security. The public and private keys serve a dual purpose: encrypting the data embedded within the watermark and facilitating its decryption during extraction. The scrambled QR watermark is then embedded into a color image using a single-level discrete wavelet transform (DWT) followed by singular value decomposition (SVD). The key plays a crucial role in this embedding process. Watermark extraction entails reversing the steps involved in embedding. The proposed method's effectiveness is evaluated through its resilience to various image-processing attacks commonly employed to remove watermarks. The authors compare their results with those achieved by state-of-the-art watermarking schemes, demonstrating that their method balances robustness (resistance to attacks) and imperceptibility (minimal visual distortion of the host image).

The burgeoning adoption of big data processing, cloud computing, and the IoT has fueled a surge in multimedia information consumption, particularly video. Within the Internet of Multimedia Things (IoMT), video is extensively streamed over communication networks, necessitating robust security measures. Unfortunately, existing methods for securing multimedia content transmission between cloud platforms and mobile devices often face limitations due to processing overhead, memory constraints, data size considerations, and battery power limitations on mobile devices. These limitations render such methods suboptimal for large multimedia files and unsuitable for the resource-restricted nature of mobile devices and cloud environments. High-Efficiency Video Coding (HEVC) is the latest video codec standard, enabling efficient storage and streaming of high-resolution videos while maintaining acceptable file sizes and superior quality. In this context, Alarifi, et al. [25] proposed a novel hybrid cryptosystem designed to safeguard the streaming of compressed HEVC video streams. This cryptosystem leverages a combination of Deoxyribonucleic Acid (DNA) sequences, the Arnold chaotic map, and Mandelbrot sets. The secure video transmission process commences with video encoding using the H.265/HEVC codec to achieve efficient compression. Subsequently, the proposed method employs the Arnold chaotic map for individual encryption of the three-color channels (Y, U, and V) within each compressed HEVC frame. Following this initial encryption step, DNA encoding sequences are established upon the resulting frames. Finally, a modified conditional shift process based on the Mandelbrot set is introduced to further obfuscate the encrypted data within the Y, U, and V channels. The authors conducted extensive simulations and security analyses to validate the proposed HEVC cryptosystem. The results demonstrate exceptional robustness and enhanced security compared to existing cryptosystems documented in the literature. This approach offers a promising solution for securing HEVC video streaming in resource-constrained environments.

IV. Results and Discussion

Because of its efficiency and speed, symmetric cryptography remains the cornerstone of digital media security. Symmetric algorithms such as AES and RC4 are widely used in content encryption, digital rights management, and secure streaming. Streaming services like Netflix use AES to protect media files during transmission and storage, ensuring that only authorized users can view the content. However, the biggest challenge is key management. The distribution and storage of secure keys represent a significant vulnerability, especially in large systems. Additionally, symmetric algorithms can be effective for real-time encryption, but their use of a single key raises security concerns if the key is compromised.

Asymmetric dual-key cryptography addresses some key management problems associated with symmetric cryptography. With public key cryptography, as demonstrated by RSA and ECC, encryption keys can be securely exchanged and content authenticity verified. Secure key exchange, digital signatures, and DRM enhancement rely heavily on asymmetric cryptography. Using asymmetric cryptography, digital certificates ensure users connect to legitimate services and media providers distribute content safely. Despite its advantages, asymmetric cryptography can be computationally intensive, which can be a problem for applications that require high-speed encryption.

Data integrity and authenticity are ensured in digital media security by hash functions. The SHA-256 feature is often used to create digital fingerprints for content, allowing unauthorized changes to be detected. Virtual signatures, blockchain content verification, and data deduplication in large media libraries are all based on hash functions. For example, blockchain technology secures digital media content by creating an immutable chain of records using hash functions. However, despite their effectiveness, hash functions have limitations. As computing power increases and new attack vectors emerge, collisions remain a problem, even with advanced algorithms like SHA-256.

The integrity and authenticity of digital content can be verified using digital signatures. In public key cryptography, digital signatures provide non-repudiation and ensure that the provenance and integrity of content can be independently verified. The review concluded that digital signatures make a significant contribution to verifying content distribution, software updates, and authentication of blockchain-based content. For example, a digital signature ensures that only legitimate software updates are distributed. This means there is no risk of devices becoming infected with malware. In resource-constrained environments, the implementation of digital signatures can be limited by the computational effort associated with signature generation and verification.

V. Challenges and Future Directions

Securing encryption keys remains one of the most significant challenges in cryptographic systems. In symmetric cryptography, securely distributing and storing keys can be problematic, especially as the number of users increases.

Although public keys can be distributed more freely in asymmetric systems, the private keys must be stored securely to prevent unauthorized access. The complexity of key management is further exacerbated in large-scale digital media systems where millions of users might be involved.

As digital media content and user bases grow, ensuring that cryptographic solutions scale effectively is crucial. High computational requirements for encryption and decryption can lead to performance bottlenecks, especially for real-time applications like live streaming. Finding a balance between robust security and system performance is essential for deploying cryptographic techniques in digital media systems.

Implementing strong cryptographic measures often introduces complexity for end-users. If accessing encrypted content or managing digital rights becomes too cumbersome, it can lead to poor user experience and lower adoption rates. Designing user-friendly cryptographic systems that provide robust security without compromising usability is a persistent challenge.

With many devices, platforms, and media formats, ensuring that cryptographic solutions are interoperable is challenging. Media content must be securely accessible across different devices and platforms without compromising security. Achieving interoperability while maintaining a high level of security requires standardization and widespread adoption of secure protocols.

Cryptographic techniques must evolve to stay ahead of emerging threats. As computational power increases, particularly with the advent of quantum computing, existing cryptographic algorithms may become vulnerable. Ensuring that cryptographic systems resist future threats is a significant challenge that requires ongoing research and adaptation.

Research into quantum-safe or post-quantum cryptography is crucial, given the potential threat of quantum computers rendering current cryptographic algorithms obsolete. Developing and standardizing cryptographic algorithms that can withstand quantum attacks will be essential for the long-term security of digital media content.

Using blockchain and other decentralized technologies can provide innovative solutions for digital media security. Blockchain can offer transparent and tamper-proof mechanisms for rights management, content distribution, and royalty payments. Smart contracts can automate and enforce access control and usage policies, reducing the reliance on centralized DRM systems.

As privacy concerns grow, incorporating privacy-preserving techniques such as homomorphic encryption, secure multi-party computation, and zero-knowledge proofs into digital media security solutions will become increasingly important. These techniques can ensure that user data is protected while still allowing necessary processing and verification.

Establishing and adopting interoperability standards for digital media cryptographic solutions can help address cross-platform compatibility challenges. Industry-wide collaboration is needed to develop and implement these standards to ensure seamless and secure access to digital media across different devices and platforms.

VI. Conclusion

In the ever-evolving digital media landscape, ensuring content security and integrity is paramount to prevent unauthorized access and piracy. This paper has provided a comprehensive overview of the cryptographic techniques for safeguarding digital media assets. The study delved into various methods to protect digital media, including encryption, DRM, watermarking, and blockchain-based solutions, starting with the fundamentals of symmetric and asymmetric cryptography, hash functions, and digital signatures. While these cryptographic techniques offer robust mechanisms to secure digital content, they also present several challenges, particularly in key management, scalability, usability, interoperability, and resistance to emerging threats. Addressing these challenges is crucial for the continued advancement and effectiveness of digital media security. Looking forward, the development of quantum-safe cryptography, enhanced key management systems, advanced DRM solutions, and privacy-preserving techniques will be essential. Integrating blockchain technology and establishing interoperability standards will further strengthen the security framework for digital media. Additionally, improving user education and simplifying the interface for secure content access will help bridge the gap between robust security measures and user convenience.

References

[1] L. Gastaldi, F. P. Appio, D. Trabucchi, T. Buganza, and M. Corso, "From mutualism to commensalism: Assessing the evolving relationship between complementors and digital platforms," Information Systems Journal, vol. 34, no. 4, pp. 1217-1263, 2024.

[2] S. Bonnet and F. Teuteberg, "Impact of blockchain and distributed ledger technology for the management, protection, enforcement and monetization of intellectual property: a systematic literature review," Information Systems and e-Business Management, vol. 21, no. 2, pp. 229-275, 2023.

[3] H. Song, N. Zhu, R. Xue, J. He, K. Zhang, and J. Wang, "Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection," Information processing & management, vol. 58, no. 3, p. 102507, 2021.

[4] K. Toshevska-Trpchevska, I. Kikerkova, E. M. Disoska, and L. Kocev, "The Importance of Intellectual Property Law in the Prevention of Selling Counterfeit Products Online," in Counterfeiting and Fraud in Supply Chains: Emerald Publishing Limited, 2022, pp. 147-169.

[5] S. Matted, G. Shankar, and B. B. Jain, "Enhanced image security using stenography and cryptography," in Computer Networks and Inventive Communication Technologies: Proceedings of Third ICCNCT 2020, 2021: Springer, pp. 1171-1182.

[6] I. Manor and E. Segev, "Social media mobility: Leveraging Twitter networks in online diplomacy," Global Policy, vol. 11, no. 2, pp. 233-244, 2020.

[7] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," Complex & Intelligent Systems, vol. 7, no. 5, pp. 2157-2177, 2021.

[8] F. Bertini, R. Sharma, and D. Montesi, "Are social networks watermarking us or are we (unawarely) watermarking ourself?," Journal of Imaging, vol. 8, no. 5, p. 132, 2022.

[9] E.-S. M. El-Kenawy et al., "Advanced dipper-throated meta-heuristic optimization algorithm for digital image watermarking," Applied Sciences, vol. 12, no. 20, p. 10642, 2022.

[10] P. Garg and R. Rama Kishore, "Comparative Analysis: Role of Meta-Heuristic Algorithms in Image Watermarking Optimization," in

Proceedings of Second Doctoral Symposium on Computational Intelligence: DoSCI 2021, 2022: Springer, pp. 315-327.

[11] B. Pourghebleh and V. Hayyolalam, "A comprehensive and systematic review of the load balancing mechanisms in the Internet of Things," Cluster Computing, pp. 1-21, 2019.

[12] B. Pourghebleh, N. Hekmati, Z. Davoudnia, and M. Sadeghi, "A roadmap towards energy - efficient data fusion methods in the Internet of Things," Concurrency and Computation: Practice and Experience, vol. 34, no. 15, p. e6959, 2022.

[13] V. Hayyolalam, B. Pourghebleh, and A. A. Pourhaji Kazem, "Trust management of services (TMoS): Investigating the current mechanisms," Transactions on Emerging Telecommunications Technologies, vol. 31, no. 10, p. e4063, 2020.

[14] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, "Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective," Sustainability, vol. 15, no. 4, p. 3317, 2023.

[15] M. A. Tofighi, B. Ousat, J. Zandi, E. Schafir, and A. Kharraz, "Constructs of Deceit: Exploring Nuances in Modern Social Engineering Attacks," in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 2024: Springer, pp. 107-127, doi: https://doi.org/10.1007/978-3-031-64171-8_6

[16] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A comprehensive study on the trust management techniques in the Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9326-9337, 2019.

[17] M. Anbari, H. Talebzadeh, M. Talebzadeh, A. Fattahiamin, M. Haghighatjoo, and A. M. Jafari, "Understanding the Drivers of Adoption for Blockchain-enabled Intelligent Transportation Systems," TEHNIČKI GLASNIK, vol. 18, no. 4, pp. 1-11, 2024.

[18] M. Harran, W. Farrelly, and K. Curran, "A method for verifying integrity & authenticating digital media," Applied computing and informatics, vol. 14, no. 2, pp. 145-158, 2018.

[19] K. Gurunathan and S. Rajagopalan, "A stegano-visual cryptography technique for multimedia security," Multimedia Tools and Applications, vol. 79, no. 5, pp. 3893-3911, 2020.

[20] M. Gafsi, S. Ajili, M. A. Hajjaji, J. Malek, and A. Mtibaa, "High securing cryptography system for digital image transmission," in Proceedings of the 8th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT'18), Vol. 1, 2020: Springer, pp. 311-322.

[21] P. William, A. Choubey, G. Chhabra, R. Bhattacharya, K. Vengatesan, and S. Choubey, "Assessment of hybrid cryptographic algorithm for secure sharing of textual and pictorial content," in 2022 International conference on electronics and renewable systems (ICEARS), 2022: IEEE, pp. 918-922.

[22] G. Panchal, D. Samanta, and S. Barman, "Biometric-based cryptography for digital content protection without any key storage," Multimedia Tools and Applications, vol. 78, pp. 26979-27000, 2019.

[23] I. Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A chaotic-based encryption/decryption framework for secure multimedia communications," Entropy, vol. 22, no. 11, p. 1253, 2020.

[24] P. V. Sanivarapu, K. N. Rajesh, K. M. Hosny, and M. M. Fouda, "Digital watermarking system for copyright protection and authentication of images using cryptographic techniques," Applied Sciences, vol. 12, no. 17, p. 8724, 2022.

[25] A. Alarifi, S. Sankar, T. Altameem, K. 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.