Wasit Journal for Pure Science

Journal Homepage: https://wjps.uowasit.edu.iq/index.php/wjps/index
e-ISSN: 2790-5241 p-ISSN: 2790-5233

Comprehensive on Exploring Advanced Ciphering for Enhanced Data Protection: Review

Nibras A.Mohammed Ali[1]*, Sajaa G. Mohammed[2], Faisel G.Mohammed[3], Firas A.Mohammed Ali[4],

[1]Department Computer Science,
College of Education for Women, University of Baghdad, Baghdad, Iraq,

[2] Department of Mathematics,
College of Science, University of Baghdad, Baghdad, Iraq

[3]Department OF Remote Sensing and Geographic Information,
College of Science, University of Baghdad, Baghdad, Iraq

[4]Center for Strategic and International Studies,
College of Science, University of Baghdad, Baghdad, Iraq

*Nibras A.Mohammed Ali:

DOI: https://doi.org/ 10.31185/wjps.265
Received 11 November 2023; Accepted 14 December 2023; Available online 13 December 2023

ABSTRACT: Steganography is the scientific practice of concealing a confidential message within a medium, without causing any noticeable alteration to the original medium. Steganography allows for the concealment of information within carrier items, such as photos, videos, sound files, and text files, throughout the process of data transmission. Within the realm of image steganography, this is a significant issue. The researchers want to enhance the capacity of concealing data within a host image without introducing any statistical anomalies. Substantial alteration. In the present digital age, where sensitive information is constantly at risk of unauthorized access, safeguarding data is of utmost importance. Methods such as ciphering and steganography are crucial for maintaining the confidentiality and authenticity of data. This study examines advanced encryption and covert communication techniques that enhance the protection of data. This review provides a comprehensive analysis of current approaches, including their benefits, drawbacks, and potential applications, through the examination of relevant research publications.

Keywords: encryption; Cyber security; open encryption; hidden communications; Encryption algorithms. convolutional neural networks; hide pictures; Steganography; Video data masking; Hide texts; electronic watermarks; Cryptanalysis. Data and information theory.

1. INTRODUCTION

1.1 Overview of data protection challenges

Data protection ensures data security and accessibility, encompassing safeguarding and maintaining operations. Techniques focus on accessibility and optimizing data administration. Data availability ensures business operations even in data degradation or loss. Data protection relies on data lifecycle and information lifecycle management, which automate data transfer and safeguard against failures, malware, virus attacks, and equipment failures[1].

Protecting data and information is of great importance in the modern era to ensure the privacy and security of personal and public information, despite the fact that life challenges in various fields are many. There are also many difficulties that are faced in different ways, some of which are shown below[2].

1. The incidence of data leakage and electronic attacks is increasing, as these violations and unauthorised access to important data lead to identity theft, financial losses, and damage to reputation [3][4].
2. Companies must comply with data protection legislation such as the California Consumer Privacy Act (CCPA) to ensure full regulation, and this requires implementing appropriate privacy protocols and practices [5][6].

3. Data minimization is increasingly difficult as data collection occurs on a large scale, requiring us to thoroughly evaluate the data for legitimate and compliant processing [7][8].
4. External sources used for various data operations by those who work to provide cloud services and third-party distributors, which increases security risks. This requires organizations and their contractors to have strong data protection mechanisms [9].
5. Organisations must ensure that users are aware of data processing and have the ability to reject, consent to, or withdraw it, although consent is complex [3].
6. The mechanism to ensure the protection of personally identifiable information is through anonymization, aliasing techniques, and strong encryption procedures to prevent the re-identification of personal data [10].
7. In introducing employees, organisations must invest in training them to reduce human errors, ensure greater data protection, and improve the organisation's employees' understanding of different protection methods [11].
8. Ciphering (Encryption): Encryption techniques safeguard confidential information by converting it into an unreadable form, ensuring data integrity through algorithms that detect unauthorized modifications, and verifying data origin [12].
9. Importance of ciphering and steganography techniques Ciphering and steganography techniques are vital for maintaining the security and privacy of information in digital communications and data storage systems [11].
10. Steganography is Covert Communication: Steganography techniques allow for the covert transmission of confidential information, reducing suspicion and ensuring privacy by minimizing detection by unintended recipients or eavesdroppers. Protection through Occlusion: Steganography enhances security by concealing hidden information, making it undetectable during interception, thus protecting it against unauthorized intrusion. Steganography techniques are crucial for information security preservation, safeguarding sensitive data and confidentiality, and are utilized in military communications, cyber security, digital forensics, and routine digital communication [13][14].
To address these challenges, a comprehensive approach must be taken that includes robust security methods and mechanisms, privacy by design mechanisms, regular security audits, and staying current on data encryption requirements. This is a discourse on the primary research contribution, which is a comprehensive depiction of privacy research from a transdisciplinary perspective. The paper concludes after presenting this rich image[15][16].

2. CIPHERING TECHNIQUES

Cryptographic algorithms encode and decode data by transforming plaintext into ciphertext using a key. Various forms of encryption are illustrated in the figure (1):

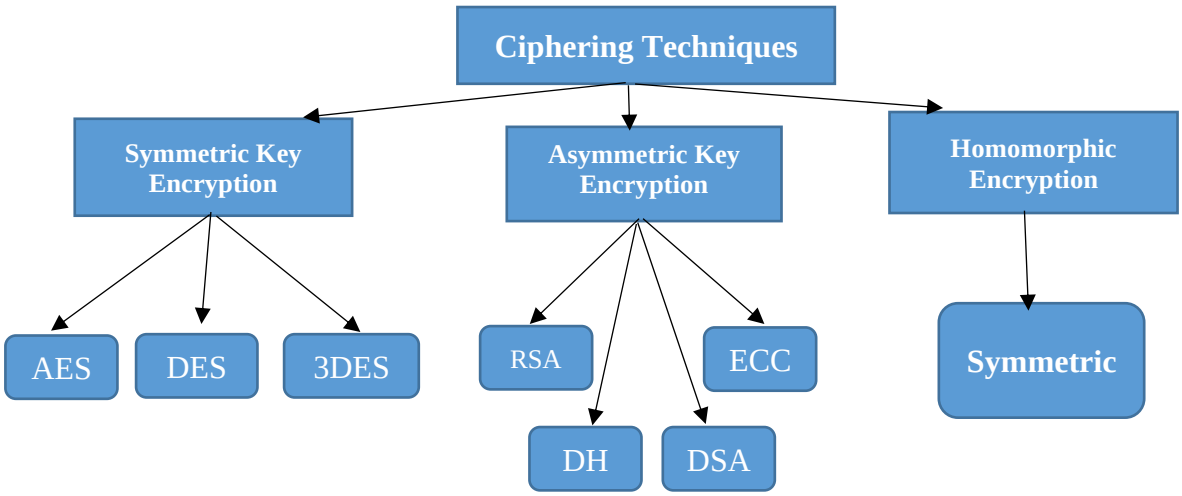

Figure (1): The Diagram Shows the Different Types of Ciphering in Addition to The Most Important Sub-Algorithms Associated with Them

2.1 Symmetric Key Encryption

Review popular symmetric key algorithms (e.g., AES, DES), There are many types of symmetric encryption shown as followed, Symmetric key algorithms are encryption methods that use the same secret key for both encryption and decryption.

1.The Advanced Encryption Standard (AES): The US government standardized AES in 2001, a block cypher encryption technology with key sizes of 128, 192, and 256 bits, known for its high security in data encryption [17].

2.The Data Encryption Standard (DES) DES, a popular 1970s and 1980s block cypher encryption technique, uses 64-bit blocks and a 56-bit key, but is now less recommended due to its small key size. [18][19].
3.The Triple Data Encryption Standard (3DES) The DES technique, which uses three distinct keys to apply the DES process to each block, enhances security but is still used in outdated systems [20][21].
4. The Two Fish encryption method, a block cypher replacing the Blowfish algorithm, supports key sizes up to 256 bits while maintaining a fixed block size of 128 bits, offering robust security measures [8].

A symmetric encryption, the key is to identify the strengths and weaknesses. The widely used method of symmetric key encryption is to use the same key for encryption and decryption operations, with strong and weak points.

Strengths:

1. The symmetric key encryption process is generally faster than the asymmetric key encryption process because it uses a single key for encryption and decryption.
2. Symmetric-key encryption is one of the easiest types of encryptions to use due to its ease of implementation and management, using a single key for both decryption and encryption operations [22].
3.Efficiency: The symmetric key encryption method is more efficient due to its advanced use of computational efficiency and resources compared to asymmetric key encryption [21].
4. Symmetric key encryption is a reliable way to protect sensitive information in data security, but only on the condition that it is used efficiently, wisely, and with a reliable and strong key [23].

Weaknesses:

1.It is extremely important to distribute keys for secure communication in the symmetric key encryption process, because the continuity of communication is effectively maintained through insecure means and this can pose challenges [13].
2.Maintaining key security is very important for symmetric key encryption, as it has become possible for a compromised key to put the security of encrypted data at risk.
3.The limitations of symmetric key encryption include non-repudiation, which makes it difficult to determine the sender of a message [24].
4.The process of expanding symmetric key encryption, due to the difficulty of managing it, is limited and the distribution of many keys is also limited, and this may pose challenges when developing the system to include larger and broader networks or systems [13].

Symmetric key cryptography is an effective, fast, simple and suitable technique for key management and distribution, but it is not suitable in cases of non-repudiation or scalability.

2.2 Asymmetric Key Encryption

Show the main common asymmetric algorithms. Public key algorithms, also known as asymmetric key algorithms, use two distinct keys for decryption and encryption and are widely used in different fields [25].
1.RSA, developed by Shamir, Rivest, and Adleman in 1977, is a well-known method of public key cryptography that uses large prime numbers to create key pairs and supports up to 4096-bit key sizes [14].
2. Elliptic Curve Cryptography (ECC) is a widely used public-key encryption method due to its efficiency and speed, particularly in mobile and embedded devices, utilizing shorter key lengths [26].
3.The Diffie-Hellman (DH) protocol is a secure cryptographic technique used for key exchange between parties, enabling mutually agreed-upon secret keys without physical exchange [27].
4.The Digital Signature Algorithm (DSA) is a public-key encryption scheme used to generate digital signatures, providing dual encryption functionality and digital signature generation alongside other techniques [26].
Popular asymmetric key algorithms consider security, size, speed, compatibility, and key management and distribution challenges when selecting, ensuring security, compatibility with existing systems, and speed [28].
Strengths and weaknesses of asymmetric key encryption. Asymmetric key encryption, also known as public-key encryption, is a widely used method that employs two distinct keys for encryption and decryption [29].

Strengths:

1. Asymmetric key encryption simplifies key distribution issues by using the public key of each party involved for encryption and the private key for decryption [30].
2. Non-repudiation: The utilization of asymmetric key encryption facilitates the achievement of non-repudiation, hence simplifying the process of establishing the identity of the message sender.
3. Asymmetric key encryption offers scalability, making it ideal for legal contexts, as it doesn't require multiple keys distribution [31].
4. Security: The use of asymmetric key encryption can provide a high degree of security for secured information, when implemented correctly and with thoughtful, strong keys.

Weaknesses:

1. Asymmetric-key encryption is slower than symmetric-key encryption. This is because two separate keys are used for encryption and decryption [32].
2. Due to the use of two different keys and the need for key management, Asymmetric key encryption becomes more complex [20].3. Maintaining key security requires asymmetric key encryption in the form of precise keys. If the private key is lost or stolen, the security of the encrypted data is also compromised [15].
4. It requires larger key sizes than symmetric key encryption and asymmetric key encryption, which makes it difficult to use on low-power devices [33].

The advantages of asymmetric key encryption are key distribution, non-repudiation, and scalability, while the disadvantages are that it may become more complex and slower, and this requires careful key management for security [34].

2.3 Homomorphic Encryption

Symmetric encryption based on basic concepts; symmetric encryption allows mathematical operations to be performed on encrypted data without the need to decrypt it. This leads to mathematical operations being performed on the ciphertext and produces the same result as the plain text [35].

• The symmetric algorithm is used in symmetric encryption, in which data is encrypted using the symmetric algorithm, and this is what makes the ciphertext incomprehensible if we lose the decryption key [36].
• The second basic element is computation, which performs mathematical operations on encrypted data without having to decrypt it. This preserves encryption and leads to encrypted results[34].
• The third and final principle of symmetric encryption is decryption, which allows the encrypted result to be decrypted using the decryption key to obtain the same result as the plain text [36].

One of the characteristics of symmetric encryption is that it provides strong data privacy and security by enabling calculations on confidential data stored on the cloud and in secure messaging applications, and this works to ensure data confidentiality and privacy without revealing information[37].

Symmetric encryption, its applications, and its limitations, Homomorphic encryption is a secure method that allows mathematical operations to be performed on encrypted data without the need for prior decryption, while emphasizing various applications and limitations [38].

1. Cloud computing employs homomorphic encryption techniques to securely process sensitive data, ensuring confidentiality and providing financial benefits to individuals and organizations [17].
2. Homomorphic encryption allows computations on encrypted data, enabling the examination of confidential information while maintaining the data's confidentiality [39].
3. Secure messaging: Homomorphic encryption is used in secure messaging applications to perform computations on encrypted communications while keeping the contents undisclosed to only the intended recipient [16].

Homomorphic encryption is beneficial in financial applications, particularly online banking, as it allows computations on encrypted data, protecting it from unauthorized access or disclosure [40].

Limitations:

1.Homomorphic encryption's computational complexity can lead to prolonged processing times for encrypted data, potentially posing limitations in real-time scenarios [15].
2.Homomorphic encryption's security relies on meticulous key management practices, but can be compromised if the private key is unlawfully obtained [41].
3.Restricted functionality: Homomorphic encryption, a relatively new technology, currently has limitations in its utility compared to traditional encryption methods.
4.Key Sizes: Homomorphic encryption, unlike standard methods, requires larger key sizes, which can pose challenges, especially when dealing with low-power devices [17].

Homomorphic encryption is a robust encryption technique with potential applications in data integrity and confidentiality sectors, but its implementation requires considering its limitations and downsides [42].

3. STEGANOGRAPHY TECHNIQUES

Steganography involves hiding information within a different message or item to evade detection, encompassing text, images, videos, and audio. It can be extracted upon reaching its intended location. Various forms of encryption are illustrated in the figure (2) [43]:

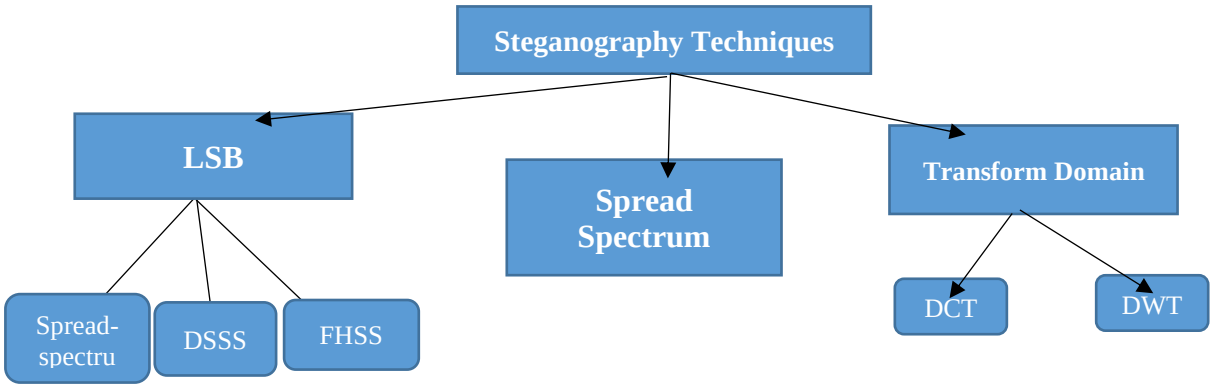

Figure (2): The Diagram Shows the Different Types of Steganography Techniques in Addition to The Most Important Methods Associated with Them

3.1 LSB Substitution

The fundamental concept behind the LSB approach is to substitute less significant components of the host picture with segments of confidential information. Presented below is a comprehensive overview of the most significant categories:

a) Overview of least significant bit (LSB) substitution technique. Spread spectrum-based steganography is a method used to conceal confidential information by dispersing it over a wide frequency range, typically in audio, image, or video files through modulation [44].

1. Spread-spectrum modulation is a communication technique that uses a pseudorandom noise pattern to distribute signal energy over a wider frequency range, ensuring confidentiality [19].
2. Direct Sequence Spread Spectrum (DSSS) is a type of communication technology that spreads the signal bandwidth by multiplying it with a pseudo-random noise sequence [19]. This spreads the signal over a wide bandwidth.
3. Spectrum-based Frequency Hopping Spread Spectrum (FHSS) steganography changes the signal in a way that looks like a pseudo-random sequence. This makes it hard to hack, very safe, and very unlikely to be found [45].
4. Limitations of spectrum-based steganography include good signal-to-noise ratio, need for a secret key, and limited ability to hide data within cover media [19].

Spread spectrum-based steganography provides strong security although steganography requires practical implementation to address potential limitations, by distributing secret information across different frequencies.

Limitations and effectiveness

It can be defined as spread spectrum based, a method of hiding confidential data by spreading it over a wide frequency band, with the ability to analyze its effectiveness and limitations[46].

effectiveness:

1. Due to its wide distribution and difficulty of detection, spectrum-based steganography provides high security, which makes it difficult for attackers to distinguish between coverage media and steganographic data [20].
2. Steganography is resistant to attacks such as compression, visual inspection, and statistical analysis due to the difficulty of locating hidden data within the cover media [18].
3. Due to the wide bandwidth, spread spectrum-based steganography has a low probability of detection, which makes it difficult for attackers to detect the presence of hidden data [20].

Limitations:

1. In steganography If the secret key is compromised, the security of the hidden data will also be compromised. It is a spectrum-based use of a secret key to generate a pseudorandom sequence that is used to distribute secret data across a cover medium [47].
2. For spectrum-based steganography to be effective, it needs a large spread of signal-to-noise ratio. If the signal-to-noise ratio is insufficient, this makes it difficult to extract hidden data from the middle of the envelope [15].
3. Its ability to hide information in the middle of the cover is limited. The reason for this is that the amount of confidential data that can be hidden must be widely spread.
4. Spread spectrum-based steganography is vulnerable to signal processing techniques such as resampling, compression and filtering which can alter the pseudorandom sequence used to distribute secret data [16].

Spread spectrum-based steganography offers high security and attack resistance, but has limitations such as secret key requirement, high signal-to-noise ratio, and limited data capacity [47].

3.2 Spread Spectrum Technique

Review of spread spectrum-based steganography; Spread spectrum-based steganography uses spread spectrum modulation technique to conceal sensitive information in a cover medium like audio, image, or video file across a broad bandwidth.

1. Steganography based on the spread spectrum uses pseudorandom noise sequence to distribute signal energy across a broad bandwidth, while confidential data is distributed across the cover medium [21].
2. Spread spectrum modulation involves spreading the spectrum in direct sequence using a pseudorandom sequence, compounded to disperse it across a broad bandwidth [19].
3. Spread spectrum modulation: Spread spectrum modulation uses pseudorandom noise to distribute signal energy across a broad bandwidth, while a secret key generates a pseudorandom sequence for confidential data distribution [21].
4. Spread the spectrum in direct sequence: This spread spectrum modulation uses a pseudorandom sequence to modulate the signal, which is then compounded to disperse it across a broad bandwidth [19].
5. Frequency-hopping spread spectrum: Spread spectrum modulation uses a pseudorandom sequence to alter signal frequency, offering high security, resistance to assaults, and low discovery risk in steganography [21].
6. Spread spectrum-based steganography has disadvantages such as a high signal-to-noise ratio, the need for a secret key, and limited data hiding in the middle of the envelope.

Spread spectrum-based steganography is a secure way to hide confidential information by distributing it across different frequencies, but it has limitations that require careful consideration [48].

Advantages and disadvantages of spread spectrum technique

Spread spectrum technology is a signal modulation method that distributes signal energy across different frequencies, and this leads us to present its advantages and disadvantages.

Advantages:

1. Spread-spectrum technologies provide extended security by dispersing signals across a large frequency range, making them difficult to jam or detect [20].
2. It shows resistance against various forms of interference, such as intentional interference, multipath interference, and frequency-selective fading.
3. Spread spectrum techniques optimize bandwidth utilization by allowing multiple signals to coexist within the same frequency band without interference [15].
4. Spread spectrum techniques can enhance signal quality by reducing interference and noise impact.

Disadvantages:

1. Spread spectrum techniques are more complex than conventional modulation methods, requiring additional hardware and software.
2. Cost: The system's cost may increase due to the additional hardware and software required for deploying spread spectrum techniques[14].
3. Power usage: Spread spectrum approaches, which use more power than conventional modulation techniques, may pose issues for battery-operated devices.
4. Limited capacity: Compared to some other modulation techniques, spread spectrum approaches have a limited capacity for data transmission [17].

Spread spectrum techniques offer high security and interference resistance, but are complex, costly, and require more power, potentially affecting battery-powered devices and data capacity [49].

3.3Transform Domain Techniques

Examination of transform domain-based steganography (e.g., DCT, DWT), This paper examines transform domain steganography techniques, which conceal confidential information by transforming cover mediums into specific forms like images, audio, or video files using the discrete cosine transform, a widely used mathematical technique in steganography and photo compression [18].

1. The discrete wavelet transform (DWT) is a widely used transform in steganography and signal processing, used to conceal data by modifying cover media coefficients imperceptibly [14].
2. Transform domain-based steganography offers enhanced security, resilience to signal processing processes, and substantial data concealment capacity within the cover medium [18].
3. Limitations: Domain-based steganography techniques have limitations such as the need for a suitable cover medium, a high signal-to-noise ratio, and limited resilience to certain signal processing operations [19].
4. Transform domain-based steganography uses methods like LSB replacement, QIM, and histogram shifting to conceal confidential information, offering security but with limitations, commonly encoding DCT and DWT.

b) Comparative analysis of different transform domain techniques

Steganography utilizes transform domain techniques like DCT, DWT, and DFT, with DCT being a widely used transform in photo, video, and steganography.

1. DCT in steganography effectively conceals data but is vulnerable to statistical analysis attacks and signal processing techniques like cropping or scaling [22].
2. The discrete wavelet transform (DWT) is a widely used steganography and signal processing method, offering security and robustness in compression and filtering but being more challenging to implement and less effective in data concealment [22].
3. DFT analysis of frequency subcomponents of signals offers enhanced confidentiality and resilience, but its adoption is limited compared to DCT or DWT-based steganography methods, which offer lower information hiding capabilities [23].
4. DWT and DCT-based steganography techniques use quantization index modulation to encode confidential information, providing robust security but vulnerable to statistical analysis attacks due to limitations in data concealment [21].

Steganography employs DCT, DWT, and DFT transformations, with Quantization Index Modulation (QIM) being a popular method but susceptible to statistical analysis attacks.

4. ADVANCED CIPHERING TECHNIQUES

Symmetric encryption is a method that use a single key for both encrypting and decrypting secure data. Data undergoes multiple iterations of substitution, transposition, and mixing to enhance its resistance against compromise, rather than being encrypted only once [50].

4.1 Quantum Key Distribution (QKD)

Introduction quantum key distribution,Quantum key distribution (QKD) is a secure communication method using photons to represent binary numbers. It allows Alice and Bob to create a secret key, even with an eavesdropper present, due to the receiver's ability to detect interceptions [19]. Evaluation of QKD's potential for enhanced data protection
Quantum key distribution (QKD) offers enhanced data protection and communication security due to various factors, making it a promising solution for data protection.

1. Quantum key distribution (QKD) offers robust security due to quantum physics laws, ensuring immediate detection of potential communication interception, making it impervious to various attacks [25].
2. Key distribution: Quantum Key Distribution (QKD) creates a confidential cryptographic key between two entities, ensuring safe communication due to its random nature and protection against unauthorized interference [24].
3. Key Renewal: Quantum Key Distribution (QKD) ensures the periodic renewal of a secret key, preventing unauthorized access and rendering it ineffective for future communication purposes.
4.Application versatility: Quantum Key Distribution (QKD) is crucial in fields like banking, military, and healthcare for protecting data integrity [25].

However, there are some limitations to QKD that need to be considered:

1.The cost of quantum key distribution (QKD) technology remains relatively high in comparison to conventional encryption methods, hence posing a potential obstacle to its extensive implementation.

2.The deployment of QKD necessitates a specialized infrastructure, posing difficulties in terms of establishment and upkeep [26].
3.One of the drawbacks of quantum key distribution (QKD) is its distance restrictions, as the communication distance is constrained by the loss experienced in the transmission medium. The limitations of its use in some applications can be observed.
4.Technical problems: Quantum Key Distribution (QKD) is a sophisticated technique that presents several technical obstacles that need to be addressed. These challenges mostly involve enhancing the efficiency and dependability of QKD systems [24].

Quantum Key Distribution (QKD) offers enhanced data and communication security, but faces financial, infrastructure, and geographical limitations. Despite these, it's a promising technology with potential for further development.

4.2 Fully Homomorphic Encryption (FHE)

Overview of fully homomorphic encryption, Fully Homomorphic Encryption (FHE) is a cryptographic technique that enables computations on encrypted data without decryption, potentially revolutionizing data security and privacy[12].

Fully Homomorphic Encryption (FHE) is a cryptographic framework that uses lattice cryptography to encrypt data using a public key and homomorphic operations, resulting in an encrypted value that can be decrypted using a private key [17]. Federated learning of heterogeneous ensembles (FHE) exhibits numerous possible applications, which encompass:

1.The use of Fully Homomorphic Encryption (FHE) in cloud computing enables the execution of calculations on encrypted data, ensuring a robust level of security and privacy for confidential information.
2.Fully symmetric encryption (FHE) is an encryption technology that enables secure sharing of data across multiple parties by keeping key information confidential.
3. One of the potential applications of fully homomorphic encryption (FHE) is in the field of machine learning, where it can be used to perform mathematical operations on encrypted data within machine learning models.
Homomorphic encryption (FHE) provides protection for sensitive data and a great deal of privacy, but its widespread application faces challenges such as overcoming obstacles:

1. Computational operations on encrypted data tend to be slow and require resources. The performance of fully homomorphic encryption (FHE) is computationally intensive.
2. Implementing fully homomorphic encryption (FHE) requires specialised skills and deep understanding due to its complex nature [27].
3. Key management is a critical aspect of implementing fully symmetric encryption (FHE).
FHE can improve data privacy and security, as managing public and private keys in large-scale systems is a major challenge, but it requires problem solving before widespread use.[23]

Challenges and advancements in FHE implementation, Fully Homomorphic Encryption (FHE) offers potential for encryption, but challenges persist. This discourse discusses obstacles and breakthroughs in implementing FHE for widespread adoption.

1. Through advances in algorithms and implementation techniques, the performance of fully homomorphic encryption (FHE), such as parallel computing optimisation and SIMD instructions, has been improved to reduce computational effort, time, and resource burdens.
2. Implementing fully homomorphic encryption (FHE) requires specialised knowledge due to its complexity. Progress has been made, with high-level APIs and key management becoming crucial aspects, enhancing ease of use for developers [22].
3. Key management systems for fully homomorphic encryption (FHE) have made significant progress, employing key rotation methodologies for secure cryptographic key administration across a given period. [25].
4. Fully Homomorphic Encryption (FHE) introduces noise into encrypted data, potentially deteriorating its quality. However, advancements in FHE algorithms, such as bootstrapping methodologies, have effectively mitigated noise accumulation, improving data quality [11].
5. Fully Homomorphic Encryption (FHE) adoption is a young technology with limited resources and skills. The Homomorphic Encryption Standardization Consortium (HESC) aims to establish standardized guidelines and protocols for FHE implementation. [18].

In brief, Fully Homomorphic Encryption (FHE) implementation faces challenges like performance, complexity, and noise buildup. However, progress has been made through enhanced algorithms, methodologies, and management strategies, resulting in improved performance and usability.

5. ADVANCED STEGANOGRAPHY TECHNIQUES

Steganography involves hiding information within a different message or item to evade detection, encompassing text, images, videos, and audio, which is then extracted upon reaching its intended location.

5.1 Adaptive Steganography

Discussion on adaptive steganography methods, Adaptive steganography is a technique that customizes the embedding process to the cover medium's characteristics, enhancing the security of concealed messages. It involves using a cover media model to determine the upper limit of concealable data, considering factors like color distribution and image texture, to determine the most suitable positions and quantities of data to be concealed [9]. Adaptive steganography techniques enhance security and resilience by dynamically adjusting hiding capacity, particularly in cases of significant variability or noise interference. However, these methods can be more complex and processing-intensive than non-adaptive methods, limiting their feasibility in specific contexts [49].
Analysis of their effectiveness against detection algorithms, Adaptive steganography techniques, such as picture and audio steganography, customize message concealment, increasing complexity for adversaries, and minimizing perceptual effects [27]. Steganographic techniques cannot guarantee complete security, and advancements in detection algorithms

continue. Adaptive techniques may be more effective, but they are susceptible to detection threats. The effectiveness of any steganographic technique depends on the algorithm, message size, and media characteristics, making it crucial to assess its effectiveness in specific environments [9].

5.2 Deep Learning-based Steganography

Deep learning techniques for hiding information, it is a technique that involves training neural networks to learn complex data representations, as deep learning techniques have shown promising results in the science of data hiding. These networks are used in tasks like image and audio processing, natural language processing, and speech recognition, identifying optimal data embedding locations and amounts to minimize perceptual impact [28]. GANs, a deep learning approach for steganography, involve a generator and discriminator trained in a game-like environment. The generator creates realistic steganographic images, while the discriminator distinguishes between steganographic and non-steganographic signals are used for image processing to learn embedding processes, minimizing perceptual quality impact. While deep learning techniques for steganography are still in development, they show promise for improving security and robustness. However, evaluation of their effectiveness in specific contexts and awareness of potential vulnerabilities are crucial [29].

Evaluation of their performance and robustness, Deep learning techniques for steganography are evaluated based on their ability to conceal information, perceive the medium, and resist attacks. The concept of hiding capacity measures the amount of data concealed while maintaining acceptable perceptual quality, using metrics like PSNR and SSIM [9]. Steganographic systems' resistance to detection assaults is assessed using metrics like detection error rate and false positive rate, while deep learning techniques maintain confidentiality of concealed data [25]. In general, Deep learning methods' effectiveness in steganography depend on neural network complexity, hidden message size, and medium properties, requiring thorough assessment and experimentation to determine resilience.

6. COMPARATIVE ANALYSIS AND EVALUATION

Comparison of advanced ciphering and steganography techniques. Advanced ciphering and steganography techniques are used to protect sensitive information from unauthorized access or detection. Ciphering transforms plaintext messages into ciphertext using a cryptographic algorithm and secret key, allowing secure transmission or storage. Techniques like AES and RSA provide strong encryption and protect data from unauthorized access. However, ciphering techniques do not hide the data's existence, making them effective in preventing unauthorized access [25]. Steganography, a non-technical approach to data protection, conceals messages in cover mediums like images, audio signals, or text documents, requiring a secret key for recovery. Advanced ciphering and steganography techniques provide robust encryption and data protection, with the choice depending on application requirements and data nature [28].

The text discusses the use of ciphering and steganography techniques in applications, discussing potential drawbacks and security requirements that may influence the choice.

Assessment of their strengths, limitations, and trade-off

Assessment of strengths, limitations, and trade-offs can be applied to various topics, such as technologies, methodologies, or even individuals. Here are some possible examples [41]:

1. Artificial Intelligence (AI)
   - AI excels in handling large data volumes, executing complex tasks, and acquiring knowledge through experience, enhancing performance as it progresses.
   - Limitations: Artificial intelligence (AI) may exhibit biases or produce erroneous outcomes when it lacks enough training or supervision. Moreover, it is susceptible to potential attacks or manipulation.
   - Trade-offs: AI's potential for enhanced efficiency in employment can be a potential risk, but it also raises ethical concerns about potential discriminatory practices [5].

2.Agile Development Methodology
   - One of the notable strengths of agile development is its ability to provide flexibility and reactivity in adapting to evolving requirements or shifting priorities. It fosters a culture of collaboration and facilitates effective communication among team members.
   - Limitations: The agile development approach may not be suitable for projects characterized by stringent deadlines or highly rigid criteria. Scaling up for larger enterprises or organizations can present challenges [20].
   - Trade-offs: The adoption of an agile strategy necessitates a fundamental transformation in the organizational culture and may not be universally applicable to all project types or teams.

3.Personal Productivity
   - Being productive allows individuals to achieve their goals, experience fulfillment, improve time management, and maintain a healthy balance between professional and personal spheres.
   - Limitations: Excessive production focus can lead to burnout, disregard for well-being, and impractical expectations, posing a burden on maintaining high productivity levels [22].

Balancing production with self-care and relaxation can be challenging due to trade-offs. Success requires setting achievable goals, prioritizing tasks, and considering personal needs and constraints.

Assessing the advantages and disadvantages of a method or technological advancement is crucial, as finding a universally applicable solution is rare due to varying circumstances. Identification of potential synergies between different techniques can lead to more effective and efficient solutions. Here are some examples of potential synergies:

4.Artificial Intelligence (AI) and Human Expertise: - AI can analyze large datasets, providing complex insights, but can also generate biased judgments. Organizations can leverage AI's synergy with human expertise to enhance decision-making and identify potential challenges [24].

5.Agile Development and Design Thinking: - Agile development and design thinking are key methodologies in addressing evolving requirements, fostering adaptability and user-friendly products or services through rapid iteration and testing of solutions [27].

6.Lean Manufacturing and Six Sigma: - Lean manufacturing and Six Sigma are methodologies that enhance production processes, reduce waste, and minimize defects, thereby improving quality, cost reduction, and customer satisfaction.

7.Mindfulness and Cognitive Behavioral Therapy (CBT): - Mindfulness and cognitive-behavioral therapy (CBT) are therapeutic approaches that enhance self-awareness and master cognitive processes and emotional states by identifying and modifying negative thought patterns [15].

Identifying potential synergies among strategies involves assessing strengths and limitations of each approach, integrating them mutually, and potentially improving problem-solving efficiency by leveraging multiple methodologies.

7. APPLICATIONS AND FUTURE DIRECTIONS

Review real-world applications of advanced ciphering and steganography. Advanced ciphering and steganography are methodologies employed to safeguard information through the process of encoding, rendering it arduous to decrypt or detect. The following are examples of practical applications of these concepts in real-world contexts:

1. Advanced encryption techniques and steganography enhance communication security, ensuring confidentiality and integrity of information between individuals and organizations, including military and governmental entities [9].

2. Digital watermarking is a steganography technique used by stock photography websites to discreetly embed a digital watermark within images or videos, identifying the media's rightful owner [1].

3. Steganography is a method to protect copyrighted content by embedding a message or copyright details in an unassuming medium, effectively deterring unauthorized use or distribution.

4.The aforementioned method can be employed for the purpose of surreptitiously transmitting information across security checkpoints or safeguarding confidential data from unauthorized access [28].

5. Sophisticated encryption techniques and steganography can be used to obfuscate data or alter evidence, posing challenges for forensic analysts in identifying or retrieving original material. This method can be used by individuals involved in illicit activities or acts of terrorism to conceal their actions or to protect personal identity.[28].

Advanced ciphering and steganography have lawful applications but can also be used for illicit or malevolent purposes, necessitating judicious use in line with moral principles

Emerging trends and future research directions

The field of technology is characterized by a continuous evolution of emerging trends and future research paths. Presently, several areas of attention have gained significant traction.

1. Research in AI and machine learning focuses on improving algorithms and models for complex tasks with precision and efficiency. Interest is growing in AI systems that can learn from limited data points and exhibit interpretability and transparency. The development of AI systems is also emphasized for their ability to acquire knowledge from a limited number of data points [10].

2. The Internet of Things (IoT) is a network of interconnected objects that transmit and receive data via the internet. Current research focuses on improving data transmission and processing methods for efficiency and safety, as well as exploring new applications in sectors like healthcare, transportation, and smart cities [35].

3. Blockchain technology is a secure, decentralized digital ledger used for transaction storage and tracking. Current research focuses on its potential applications in finance, supply chain management, and voting systems. The interest is growing in blockchain systems with enhanced efficiency and scalability [5].

4. The increasing integration of technology in daily life is driving the demand for cybersecurity, with current scholarly focus on developing methodologies for identifying and mitigating cyber threats and creating new tools for network and data protection.

5. Quantum computing is a rapidly growing field that utilizes quantum physics principles to perform computational tasks, with current research primarily focused on improving its capabilities to enhance computational power and efficiency.

Researchers are exploring quantum computing's applications in cryptography and pharmaceutical research, ensuring responsible and ethical use amidst the constantly evolving technology field.[30]

8. CONCLUSION AND FUTURE WORKS

Summary of key findings from the literature review:
1. Research Gaps: Literature reviews can indicate areas within the research that have not been thoroughly examined or necessitate additional examination.
2. Literature surveys may also reveal divergent outcomes or incongruous findings across several studies, underscoring promising avenues for future investigation.
3. Prospective Research Directions: Conducting literature reviews might unveil potential avenues for future research, encompassing unexplored methodologies or technologies that have yet to be thoroughly investigated.
4. Literature reviews can also serve the purpose of identifying developing trends within a particular discipline, encompassing novel fields of research as well as shifts in research methodology or approaches.
5. The current research has some limitations that can be identified through literature reviews. These limitations encompass factors such as limited sample sizes, biased samples, and incorrect methodology.
A literature review's primary outcomes depend on the research inquiry and study selection, but it can provide valuable insights into current research trends, gaps in existing literature, and potential future research directions.
Recommendations for further research and development. The identification of appropriate recommendations for additional research and development is contingent upon the particular subject matter under investigation. Nevertheless, presented here are a few overarching suggestions that could potentially be applicable across several research domains:
1. The identification of gaps in the existing literature is a common outcome of literature reviews, indicating areas of research that have not been well investigated or necessitate additional examination. Researchers have the ability to priorities the resolution of these gaps by doing novel studies or devising innovative approaches to address these specific areas.
2. It is imperative to increase the sample sizes in various studies, as a significant number of them possess restricted sample sizes, hence potentially lacking representativeness of broader populations. Researchers may choose to priorities the expansion of sample sizes in order to enhance the generalizability of their findings.
3. Longitudinal studies offer a more comprehensive understanding of phenomena over time, compared to cross-sectional designs, allowing researchers to investigate temporal variations and produce a more thorough understanding of a particular topic.
4. Researchers have the opportunity to investigate and examine novel procedures and technologies that arise, enabling them to effectively tackle current research inquiries or formulate fresh research inquiries.
5. It is imperative for researchers to contemplate the ethical ramifications of their work as technology progresses. Researchers should place a high priority on the examination of the ethical consequences associated with their work as well as the establishment of ethical rules to govern future research endeavors.
The literature review explores advanced encryption and steganography methods for data security, aiming to fill gaps, increase sample sizes, conduct longitudinal studies, investigate innovative technologies, and consider ethical considerations.

REFERENCES

[1] Jingxuan,Jing, Yue Li, "Establishing an International Engagement Model of Digital Identity Based on Blockchain," Mobile Information Systems, vol. 2022, 2022.

[2] Abdul-Jabbar S.S., Abed A.E., Mohammed S.G., Mohammed F.G.," Fast 128-bit Multi-Pass Stream Ciphering Method," Iraqi Journal of Science, 64 (5) , pp. 2589-2600.2023.

[3] Mohammed F.G., Athab S.D., Mohammed S.G.," Disc damage likelihood scale recognition for Glaucoma detection," Journal of Physics: Conference Series, 2114 (1) , art. no. 012005.2021

[4] Mohammed, F.G., Athab, S.D., "Disc damage likelihood scale recognition for Glaucoma detection,"*Journal of Physics: Conference Series*, 2021, 2114(1), 012005

[5] Christopher G. Bradley, "Privacy for Sale: The Law of Transactions in Consumers' Private Data," Yale Journal on Regulation, vol. 40, pp. 127 - 196, December 2023.

[6] P. Jiang, D. Ergu, F. Liu, Y. Cai, and B. Ma, "A Review of Yolo Algorithm Developments," Procedia Comput. Sci., vol. 199, pp. 1066–1073, 2021, doi: 10.1016/j.procs.2022.01.135.

[7] Mohammed S.G., Abdul-Jabbar S.S., Mohammed F.G.," Art Image Compression Based on Lossless LZW Hashing Ciphering Algorithm," Journal of Physics: Conference Series, 2114 (1) , art. no. 012080.2021

[8] Mohanaiah, P., P. Sathyanarayana, and L. GuruKumar. "Image texture feature extraction using GLCM approach." International journal of scientific and research publications 3, no. 5 (2013).

[9] Haibin,Chen, Jinyin,Shangguan, Wenchang Zheng, "GONE: A generic O(1) NoisE layer for protecting privacy of deep neural networks," Computers and Security, vol. 135, December 2023.

[10] Mohammed S.G., Abdul-Jabbar S.S., Mohammed F.G.," Art Image Compression Based on Lossless LZW Hashing Ciphering Algorithm," Journal of Physics: Conference Series, 2114 (1) , art. no. 012080.2021

[11] George LE, Hassan EK, Mohammed SG and Mohammed FG, " Selective image encryption based on DCT, hybrid shift coding and randomly generated secret key". Iraqi J Sci 61(4):920–935.2020

[12] Katoch, Sourabh, Sumit Singh Chauhan, and Vijay Kumar. "A review on genetic algorithm: past, present, and future." Multimedia tools and applications 80 (2021): 8091-8126.

[13] Ahmed Kamil Hasan,Alkhasraji, Jafaar Mohammed Daif Al-Ali, "Colour image encryption based on hybrid bit-level scrambling, ciphering, and public key cryptography," Bulletin of Electrical Engineering and Informatics, vol. 12, pp. 1607 - 1619, 2023.

Dutta H, Das RK, Nandi S, Prasanna SM. An overview of digital audio steganography. IETE Technical Review. 37(6):632-50.,2020

[14] M. M. Hoobi, S. S. Sulaiman, I. A. AbdulMunem, "Enhanced Multistage RSA Encryption Model," 2nd International Scientific Conference of Al-Ayen University (ISCAU), IOP Conf. Series: Materials Science and Engineering, p. 455, 2020.

[15] Ogundokun RO, Awotunde JB, Adeniyi EA, Ayo FE. Crypto-Stegno based model for securing medical information on IOMT platform. Multimedia tools and applications.80:31705-27,2021

[16] Mohammed A. Kareem and Suhad Malallah Kadhem, "Text Steganography Method Based On Modified Run Length Encoding," Iraqi Journal of Science, vol. 57, pp. 2338-2347, 2022.

[17] Mohammed, F.G., Athab, S.D., "Disc damage likelihood scale recognition for Glaucoma detection,"Journal of Physics: Conference Series, 2021, 2114(1), 012005

[18] A. Kanhe, G. Aghila, C. Y. S. Kiran, C. H. Ramesh, G. Jadav and M. G. Raj, "Robust Audio steganography based on Advanced Encryption standards in temporal domain," 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, India, 2015, pp. 1449-1453, doi: 10.1109/ICACCI.2015.7275816.

[19] Hind S. Harba,ets Eman S. Harba, "Improving Security of the Crypto-Stego Approach using Time Sequence Dictionary and Spacing Modification Techniques," Iraqi Journal of Science, vol. 62, p. 5, 2021.

[20] Makhdoom I, Abolhasan M, Lipman J. A comprehensive survey of covert communication techniques, limitations and future challenges. Computers & Security. 2022 Sep 1;120:102784.

[21] Ali, A.H., George, L.E., Zaidan, A.A. and Mokhtar, M.R., 2018.

[22] High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain. *Multimedia Tools and Applications*, *77*, pp.31487-31516.

[23] Ch.,Greeshmanth Rupa, "Novel secure data protection scheme using Martino homomorphic encryption," Journal of Cloud Computing, vol. 12, 2023.

[24] Munuera C. ,"Steganography and error-correcting codes", (Signal Processing 87 (2007) 1528–1533 ,2007, doi:10.1016/j.sigpro.2006.12.008

[25] Maytham A. Ali Nehad Hameed Hussein, "Medical Image Compression and Encryption Using Adaptive Arithmetic Coding, Quantization Technique and RSA in DWT Domain," Iraqi Journal of Science, vol. 63, 2022.

[26] Hasan A. Kazum , Faisel G. Mohammed, "White blood cell recognition via geometric features and naïve bays classifier", International Journal of Engineering & Technology, 7 (4) (2018) 3642-3646

[27] Xin,Xu, Yang,ets Liu, "The secure judgment of graphic similarity against malicious adversaries and its applications," Scientific Reports, vol. 13, 2023.

[28] George LE, Hassan EK, Mohammed SG and Mohammed FG, " Selective image encryption based on DCT, hybrid shift coding and randomly generated secret key". Iraqi J Sci 61(4):920–935.2020

[29] Haibo,Wen, Yanchuan and etc Tian, "Lattice based distributed threshold additive homomorphic encryption with application in federated learning," Computer Standards and Interfaces, vol. 87, 2023.

[30] Hussein A. M. , Al-Momen S. " Linear Feedback Shift Registers-Based Randomization for Image Steganography", Iraqi Journal of Science, Vol. 64, No. 8, pp: 5031-5046,2023 DOI: 10.24996/ijs.2023.64.8.34

[31] Jiaqi,Zhu, Hui and Wang, Fengwei Zhao, "Efficient and privacy-preserving tree-based inference via additive homomorphic encryption," Information Sciences, vol. 650, 2023.

[32] Oscar,Guijarro-Berdiñas, Bertha,Hernández-Pereira, Elena Fontenla-Romero, "FedHEONN: Federated and homomorphically encrypted learning method for one-layer neural networks," Future Generation Computer Systems, vol. 149, 2023.

[33] Alexander G. Chefranov, "Adaptive to pixel value and pixel value difference irreversible spatial data hiding method using modified LSB for grayscale images," Journal of Information Security and Applications, vol. 70, 2022.

[34] Mohamed, N. A., and M. S. H. Al-Tamimi. "Image fusion using a convolutional neural network." *Solid State Technol* 63.6 (2020).

[35] Rohit,Saluja, Deepak and Kumar, Suman Singh, "Spread Spectrum Coded Radar for R2R Interference Mitigation in Autonomous Vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 23, 2022.

[36] Samer,Alsaraira, Amer Alabed, "Implementing and developing secure low-cost long-range system using speech signal processing," Indonesian Journal of Electrical Engineering and Computer Science, vol. 31, 2023.

[37] Mohammed Ali, Firas Amer, and Mohammed SH Al-Tamimi. "Face mask detection methods and techniques: A review." *International Journal of Nonlinear Analysis and Applications* 13.1 (2022): 3811-3823.

[38] Elhadi,Abed, Djamel and Bouchemel, Ammar Mehallel, "Efficient Transmission of 2D Chaotic Maps Encrypted Images with DWT-Based SC-FDMA LTE System," Periodica polytechnica Electrical engineering and computer science, vol. 66, 2022.

[39] Nagi H.,Al Soufy, Khaled A. M. Al-Ashwal, "Performance analysis of wireless compressed-image transmission over DST-based OFDMA systems," Eurasip Journal on Wireless Communications and Networking, vol. 2023, 2023.

[40] Mohamed, N. A., and M. S. H. Al-Tamimi. "Image fusion using a convolutional neural network." Solid State Technol 63.6 (2020).

[41] Tony,Renner, Renato Metger, "Security of quantum key distribution from generalised entropy accumulation," Nature Communications, vol. 14, 2023.

[42] Yuan,Zhao, Yongli ets Cao, "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet," IEEE Communications Reviews and Tutorials, vol. 24, 2022.

[43] Yichen,Chen, Ziyang,ets Zhang, "Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber," Physical Review Letters, vol. 125, 2020.

[44] Wencheng,Wang, Song and Cui, Hui Yang, "A Review of Homomorphic Encryption for Privacy-Preserving Biometrics," Sensors, vol. 23, 2023.

[45] Shahid,Uddin, Jamal ets Rahman, "A Huffman code LSB based image steganography technique using multi-level encryption and achromatic component of an image," Scientific Reports, vol. 13, 2023.

[46] Jie,He, Peisong ,ets Luo, "Reversible adversarial steganography for security enhancement," Journal of Visual Communication and Image Representation, vol. 97, 2023.

[47] Mahesh, K. Michael,Pon Bharathi A. Veluchamy S., "DeepDrive: A braking decision making approach using optimized GAN and Deep CNN for advanced driver assistance systems," Engineering Applications of Artificial Intelligence, vol. 123, 2023.

[48] Macias, Dario Xavier Mieles, and Ermenson Ricardo Ordoñez Avila. "Modelos de minado de texto para la implementación de sistemas de predicción de plagio de la Universidad Técnica de Manabí." *Polo del Conocimiento* 8.6 (2023): 690-718.

[49] Nayyef, Rasha Helmi, and Mohammed SH Al-Tammi. "Skull Stripping Based on the Segmentation Models." *Journal of Engineering* 29.10 (2023): 74-89.

[50] Abd-Alzhra, Arwa Sahib, and Mohammed SH Al-Tamimi. "Lossy image compression using hybrid deep learning autoencoder based on k-mean clustering." *Design Engin* (2021): 7848-7861.