Image Ownership Protection Through Hybrid Approach

MSc Research Project
MSc Cyber Security

Aishwarya Tidke
Student ID: 22100377

School of Computing
National College of Ireland

Supervisor: Dr. Vanessa Ayala-Rivera

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Aishwarya Tidke
Student ID:	22100377
Programme:	MSc Cyber Security
Year:	2023
Module:	MSc Research Project
Supervisor:	Dr. Vanessa Ayala-Rivera
Submission Due Date:	14/12/2023
Project Title:	Image Ownership Protection Through Hybrid Approach
Word Count:	6522
Page Count:	22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	30th January 2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Image Ownership Protection Through Hybrid Approach

Aishwarya Tidke
22100377

Abstract

Protecting images from cyber attacks on social media has become a challenge as technology evolves. The growing concerns over preserving the ownership of digital photos uploaded online are addressed by this research. The study presents a novel and hybrid approach that includes techniques for frequency domain digital watermarking, such as RDWT (Redundant Discreet Wavelet Transform) and SVD (Singular Value Decomposition), as well as other techniques like XChaCha20-Poly1305 that have never been used before in relation to digital watermarking, chaotic logistic mapping, and Huffman coding that securely conceals ownership information in images, making it difficult for others to alter or steal them, especially on social media. The research embeds watermarks resistant to common modifications such as noise and compression. Experiments show that this hybrid strategy is effective at preserving image quality while also ensuring robust security, with evaluation metrics such as a Peak signal-to-noise ratio (PSNR) of 46 dB, a Structural Similarity Index (SSIM) of around 1, and resistance to noise, filtering, and JPEG compression attacks when compared to existing approaches. Overall, this research outlines improved imperceptibility and robustness by providing a scalable method of managing digital rights, stimulating additional developments in the domain of image ownership protection. The paper also notes its limitations in terms of countering increasingly sophisticated attacks and makes it suitable for a wider range of media such as video and audio.

1 Introduction

Social media networking has become popular as a platform for users to participate in and exchange multimedia content such as pictures, text, audio, and videos Soomro and Hussain [2019]. As per the statistics in 2016 by[1],around 64% of the photographer's work has been used in an unauthorized way. The increased sharing of photos on social media in the digital age has generated questions regarding the ownership and confidentiality of digital images. As photographs are transmitted without proper attribution, this widespread sharing frequently results in arguments over copyrights and sources. Furthermore, there is an increasing need to insert sensitive information as a watermark into these pictures for purposes such as covert communication, metadata tagging, or copyright verification. In today's digital landscape, balancing image quality, security, and payload capacity in digital watermarking is critical Pal et al. [2023].

[1] `https://www.pixsy.com/image-protection/protect-images-online`

This research aims to develop a robust technique that will preserve privacy and ownership of images shared over social media with better performance than previously developed methodologies in the domain. Those techniques are homomorphic transformation, RDWT, invisible zero watermarking, SVD with improved encryption techniques such as XChaChaPoly-1305, and chaotic logistic map techniques that improve the resistance of digital photographs against unlawful use and manipulation. Regardless of technical improvements, it is critical to establish procedures that maintain the integrity of the original image while also assuring high levels of security and efficiency.
Research Question:
How can a hybrid approach that integrates invisible watermarking, XChaCha20- Poly1305 encryption, chaotic logistic mapping, Huffman coding, homomorphic transformed image RDWT, and SVD be optimized to ensure secure and imperceptible embedding of confidential information within digital images, protecting image ownership and confidentiality on social media platforms?

2 Related Work

With respect to the extensive development of the Internet and multi-media technologies, digital picture watermarking has become a vital method for protecting digital content from illegal utilization and distribution. In research Allwadhi et al. [2022], a detailed survey on state-of-the-art digital watermarking techniques is carried out, highlighting watermarking domains, such as spatial and transform domains. It portrays that transform domain techniques are more robust and secure than spatial hence, in the given research, frequency domain techniques such as RDWT and SVD are utilized.

The research Kumar et al. [2023] provides a comprehensive review of existing watermarking techniques and the challenges associated with each of them. The present research focuses on embedding a watermark on RONI (Region Of Non-Interest) instead of ROI(Region Of Interest) as Mousavi et al. [2014] research suggests embedding the watermark in RONI (Region of Non-Interest) to secure ROI (Region of Interest).

2.1 Spatial domain digital watermarking

According to the study by Wang and Su [2022], spatial domain watermarking embeds the watermark directly into the image's pixel values. One of the simplest watermarking techniques in this domain is LSB (Least Significant Bit) which is used by Devi and Bharti [2022] research. It helps by utilizing LSB in MATLAB and aiming for higher PSNR and capacity. Trade-offs between data hiding and image quality could lead to future drawbacks. It is also used aligned with Canny edge detection in research provided by Faheem et al. [2023] that achieves a PSNR of roughly 53. Block segmentation, gradient calculation, convolution mask application, and LSB embedding are all part of the process; substitution box scrambling provides extra security against chaos. Nevertheless, the strategy might not be as effective against sophisticated attacks like steganalysis, compression, or content-preserving modifications. The current study decided not to use LSB because of the results' alleged lack of robustness.

Another work Sakshi et al. [2022] explores the least significant bit of steganography as a spatial domain method for text and image hiding. The method involves substituting the most important bits of the secret data for one to eight bits of the carrier image's initial component of pixels. Although simple to use, the approach has a trade-off with a low peak signal-to-noise ratio (PSNR 43.33) and a high mean square error, which suggests that the final image will have more noise.

2.2 Frequency (transform) domain digital watermarking

Ramos et al. [2023] highlights a self-embedding fragile watermarking algorithm that uses DWT to securely detect and recover from picture tampering by integrating BCH code and chaotic bits. The trade-off between imperceptibility and recovery is evident even when competitive performance is attained, and sensitivity to certain attacks such as Salt and Pepper points to possible areas where digital image security might be improved.

According to Savakar and Ghuli [2019], a hybrid strategy combines blind and non-blind watermarking approaches to improve resilience and copyright protection in the quickly changing field of digital picture watermarking. The method uses Singular Value Decomposition (SVD) and Discrete Wavelet Transformation (DWT) to integrate a hidden binary image with non-blind watermarking into an outside cover image after it has been embedded using a blind watermarking process. While not explicitly utilizing RDWT, this method's merging of DWT and SVD aligns with its ideas. The suggested method aims to solve some drawbacks, such as content-preserving changes and potential vulnerability to sophisticated attacks.

With a particular application in the medical industry, Rani et al. [2023] suggested study focuses on improving protected digital image watermarking. Although effective, the literature indicates that DCT methods may have computational costs and may degrade the effectiveness of picture data concealment, especially when it comes to low PSNR values.

2.3 Hybrid watermarking

According to studies conducted by Barlaskar et al. [2023], watermarking digital images is an essential technique for protecting copyrights in the digital domain. Their method, which combines discrete wavelet transform (DWT) and singular-value decomposition (SVD), tries to preserve image quality, provide resilience against attacks, and make watermarks undetectable. When combined with SVD, DWT outperforms traditional DWT against Gaussian noise, compression, and cropping attacks as per Çerkezi and Çetinel [2016] Finding the ideal balance between robustness and imperceptibility in these systems is still difficult, though.

Redundant Discrete Wavelet Transform was outlined by researchers as being more resilient to additive noise than wavelet. By using SVD and RDWT in the YCbCr color space, Dwivedi and Srivastava [2022] suggests image watermarking technique improves multimedia data security through undetectable embedding. Its effectiveness is demonstrated by evaluation criteria including PSNR, SSIM, and NC. The proposed methodology uses this method to insert a watermark in the LL subband which has proven to be more resistant to attacks such as Gaussian noise, salt & pepper, median filter, shift, histogram equalization, and JPEG compression according to Lagzian et al. [2011]. Nevertheless, the paper notes that there could be attacks and recommends using encryption algorithms to add extra security.

Lozada-Gonzalez et al. [2023] outlines the use of zero watermarking which would maintain the integrity and authenticity of an image. It is combined with the SHA-1 algorithm, the cellular automata CA criteria, and the spread spectrum via DS-CDMA.

With the BER (Bit Error Rate) of 0.5, It is effectively proven a good choice of methodology. Whereas, Morales-Ortega and Cedillo-Hernandez [2022] solely implements zero watermarking algorithm along with matching-pixel criterion in the spatial domain in conjunction with data concealing through bit replacement, compression, and encryption. Potential host picture distortions, susceptibility to sophisticated attacks, and computing efficiency issues are some of the challenges associated with zero-watermarking. The proposed research uses this technique as it hardly makes alterations in an original image while going through the watermarking process.

A new approach that combines discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD) for digital picture watermarking in the medical domain is presented in research by Amel Ali Alhussan [2023] To enhance security, the suggested approach utilizes several encryption levels and transformations. Testing against various attackers reveals great stability and imperceptibility findings. It represents PSNR greater than 35 dB.

2.4 Data Compression

With the help of hybrid prediction and Huffman coding, the research Sui et al. [2023] suggests a high-capacity reversible data hiding technique for encrypted images. By using picture redundancy and a hybrid prediction methodology based on the most significant bit-plane and remaining bit-planes of an original image, the method maximizes embedding capacity. Another research that proves the veracity of Huffman coding is done by Macarie et al. [2022]. This study compares the analyses of Shannon-Fano coding (SFC) with Huffman coding (HC). Theoretically, Huffman coding is the best option for symbol-by-symbol coding techniques, providing a productive means of representing symbols with probabilistic variable-length codes. Therefore, for the specified approach, the use of Huffman coding is chosen.

2.5 Chaotic Systems in Digital Watermarking

With tamper localization and recovery, the research Neena Raj and Shreelekshmi [2023] described here presents a strong picture authentication technique. To enable pixel-by-pixel authentication and provide 100% recovery of the original image if it is untampered with, the technique incorporates a very secure and fragile watermark. Incorporating chaotic sequence as a crucial element, the research clarifies the importance of increasing unpredictability in the process of choosing pixel locations for watermark embedding. The watermarking process's security is probably improved by the chaotic logistic mapping.

M et al. [2021] presents a multi-media encryption system that makes use of linear feedback shift registers (LFSR) and chaotic logistic maps. This method uses hybrid encryption techniques for video security, creative schemes like the imitating jigsaw method for chaos-based image encryption, and chaotic maps like Henon, Baker, and Arnold maps for image encryption to give the encryption algorithm the confusion and diffusion properties necessary for robustness and efficiency. Notwithstanding, shortcomings in the current encryption protocols are recognized, underscoring the necessity for enhanced encryption techniques to prevent cyberattacks. Hence, the proposed approach includes an XChaCha20-Poly1305 encryption method for the robustness of the embedded watermark.

2.6 Encryption techniques for data and images

The suggested Huffman coding-based method Singh et al. [2019] adds to the expanding body of knowledge by presenting a unique set of methods designed specifically for picture encryption. The utilization of Huffman coding offers a methodical and effective way to encode pixel data, however, spatial translation complicates the encryption procedure. The literature review does, however, also point forth possible directions for development and research.

Ayad et al. [2021] focus on determining the best chaotic map for picture encryption. Various chaotic maps, such as the Tent map, Logistic map, Sine map, and Arnold's Cat map, were investigated for their efficacy in picture encryption. The work identified the special needs provided by picture encryption, given the large size and complicated pixel interactions.

Kao et al. [2021] work presents a revolutionary approach for IoT (Internet of Things) data encryption, XChaCha20-poly1305. This solution overcomes the difficulties associated with network data encryption, particularly in the setting of unprotected networks. This algorithm is known for its speed and effectiveness in Sensor networks, providing a promising answer to the growing concerns about safe data transfer in multimedia technologies and communication networks.

The importance of encryption in preserving data confidentiality and integrity has been repeatedly highlighted by Adak et al. [2023]. It included a two-step data masking scheme, which incorporates AES 256 for initial encryption and RSA 2048 for subsequent column-level encryption at the database level. Decryption times in the double encryption process are dramatically impacted, highlighting a trade-off between greater security and computing efficiency.

2.7 Social Media Platforms and Image Manipulation Threats

The paper Karteris et al. [2023] outlines the cyber threats that are present on social media platforms. According to the paper's findings, the suggested approach and technology identify pertinent tweets about cyber security threats on Twitter with a respectable efficacy of 73%. Whereas, The Venugopal [2020] explores the complicated terrain of digital image copyright protection, including aspects of ownership, infringement detection, and legal defenses. This study gives insights into technological and legal complexities in the context of suggested research, matching with the development of novel approaches for digital image copyright protection and the global issues creators confront in defending their rights.

Reference	**Techniques Used**	**Key Aspects Evaluated**	**Metrics**	**Values**
Wang and Su (2022)	LSB (Least Significant Bit), Canny edge detection.	Strengths and trade-offs between data hiding and image quality.	PSNR.	40 dB PSNR value.
Ramos et al. (2023)	DWT, BCH code, chaotic bits.	Imperceptibility, recovery, sensitivity to attacks.	Not specified.	Competitive performance.

Reference	Techniques Used	Key Aspects Evaluated	Metrics	Values
Savakar and Ghuli (2019)	SVD, DWT.	Resilience, copyright protection, drawbacks in existing methods.	Not specified.	Not specified.
Rani et al. (2023)	DCT methods.	Protected digital image watermarking, computational costs.	PSNR values.	Effective, but with potential degradation in PSNR.
Barlaskar et al. (2023)	DWT, SVD.	Image quality, resilience against attacks, undetectable watermarks.	Not specified.	Difficult to achieve ideal balance.
Dwivedi and Srivastava (2022)	SVD, RDWT.	Multimedia data security, effectiveness.	PSNR, SSIM, NC.	Effective, but recommends additional encryption.
Lozada-Gonzalez et al. (2023)	SHA-1, cellular automata, DS-CDMA.	Maintaining integrity and authenticity of an image.	BER.	Effective with BER of 0.5.
Amel Ali Alhussan (2023)	DWT, DCT, SVD, multiple encryption levels.	Security, imperceptibility, stability.	PSNR.	PSNR greater than 35 dB.
Sui et al. (2023)	Hybrid prediction, Huffman coding.	Embedding capacity, reversible data concealing.	Not specified.	Large embedding capacity.
Macarie et al. (2022)	Shannon-Fano coding, Huffman coding.	Symbol-by-symbol coding techniques, variable-length codes.	Not specified.	Huffman coding chosen.
Neena Raj and Shreelekshmi (2023)	Chaotic sequence, tamper localization, recovery.	Pixel-by-pixel authentication, recovery of the original image.	Not specified.	Chaotic logistic mapping improves security.
M et al. (2021)	LFSR, chaotic logistic maps.	Linear feedback shift registers, chaotic maps for encryption.	Not specified.	Recognizes shortcomings in current encryption protocols.
Singh et al. (2019)	Huffman coding.	Encoding pixel data, challenges in spatial translation.	Not specified.	Offers possible directions for development.

Reference	Techniques Used	Key Aspects Evaluated	Metrics	Values
Ayad et al. (2021)	Chaotic maps (Tent, Logistic, Sine, Arnold's Cat).	Efficacy in picture encryption, and performance comparison.	Not specified.	Identifies special needs in picture encryption.

Table 1: Summary of literature review

In Table 1, a summary of the literature mentioned above is provided.

As a result of the broad literature review, a gap in comprehensive research is identified. The proposed strategy of integrated techniques to improve metrics like PSNR, SSIM, and NCC (Normalized Cross Correlation Coefficient), which balance imperceptibility and robustness, overcomes this gap.

3 Methodology

The research methodology outlined for this research is centered around a complex approach to image enhancement, watermarking, encryption, and data embedding. It uses a combination of Homomorphic transformation Khare and Srivastava [2021], chaotic logistic mapping Abu-Faraj et al. [2023], XChaCha20-Poly1305 encryption Manullang [2020], Huffman coding Sui et al. [2023], invisible watermarking, redundant discrete wavelet transforms (RDWT), and singular value decomposition (SVD) Dwivedi and Srivastava [2022]. The methodology is detailed step-by-step below:

3.1 Research methods

- **Analysis of Existing Methods:** The state-of-the-art methods for digital watermarking, steganography, data hiding, and encryption techniques were analyzed and studied in this phase. The literature review in section 2 highlighted the strengths and limitations of the existing methods which has set the foundation for the development of the proposed approach.

- **Data Preparation and Collection:** It involved searching and collecting high-resolution images which are used as cover images. The cover images are the standard images retrieved from a SIPI (Signal And Image Processing Institute) dataset (Baboon and Pepper)[2]and Mathship technologies web source (Lena, Barbara and Zelda) [3]. These are the classic images used in digital watermarking algorithms. The Grayscale and colored images are selected as Lena, pepper, Barbara, baboon, Zelda and used as classic testing images in previous research in this domain. QR code watermark images are generated as per the owner's data to represent ownership information.

- **Algorithm Development:** By the literature review, all of the described algorithms are conducted on the cover image and QR image with ownership data.

[2] `https://sipi.usc.edu/database/database.php?volume=misc`

[3] `https://www.hlevkin.com/hlevkin/06testimages.htm`

To improve image quality, a homomorphic transformation is applied to the cover image. On the other hand, the QR image, which is to be watermarked, is encrypted using the XChaCha20-Poly1305 encryption technique and randomized using a chaotic logistic map. To make the image more concise it is compressed using the Huffman coding compression algorithm. Finally, the QR image is watermarked into the cover image utilizing invisible zero watermarking RDWT (Redundant Discreet Wavelet Transform) and SVD (Singular Value Decomposition) techniques, with a focus on visual quality and attack resistance.

- **Implementation and Integration:** The developed algorithms are combined into a cohesive hybrid method and applied to a picture data collection. This process guarantees that all components are compatible with one another and operate together to fulfill the research's objectives.

- **Performance Analysis:** Rotating, compressing, adding noise, filtering, and other changes to the watermarked photos evaluate the watermarking technique's resilience and imperceptibility. As recommended by Sara et al. [2019], performance measurements like Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index (SSIM), and Normalized Cross-Correlation (NCC) are used to assess the approach's capability, robustness, and imperceptibility.

- **Comparison with Existing Techniques:** To measure the effectiveness of the optimized hybrid strategy against current encryption and watermarking techniques, a comparative analysis is carried out. This analysis emphasized the benefits of the suggested system by focusing on the trade-offs between robustness and imperceptibility.

Figure 1 depicts the high-level flow of the research approach, showing the stages from the original image and watermark QR image via different transformation and encryption methods, ending in the watermarked image.

3.2 Evaluation Strategy

The proposed approach is meant to evaluate against imperceptibility, robustness, ownership authentication, and resilience to attacks such as compression, noise addition, and filtering.

3.2.1 Imperceptibility evaluation

The first criterion for evaluating images is quality. Imperceptibility relates to whether or not the watermark is visible on the cover image to maintain the quality of the watermarked image. As stated below, measurements like PSNR (Peak Signal-to-Noise Ratio), Mean Squared Error (MSE), and SSIM (Structural Similarity Index) can be used to compute these.

- **Peak Signal-to-Noise Ratio (PSNR)**

The PSNR (Peak Signal-to-Noise Ratio) compares the quality of the watermarked image to the original image. It computes the similarity between a watermarked image

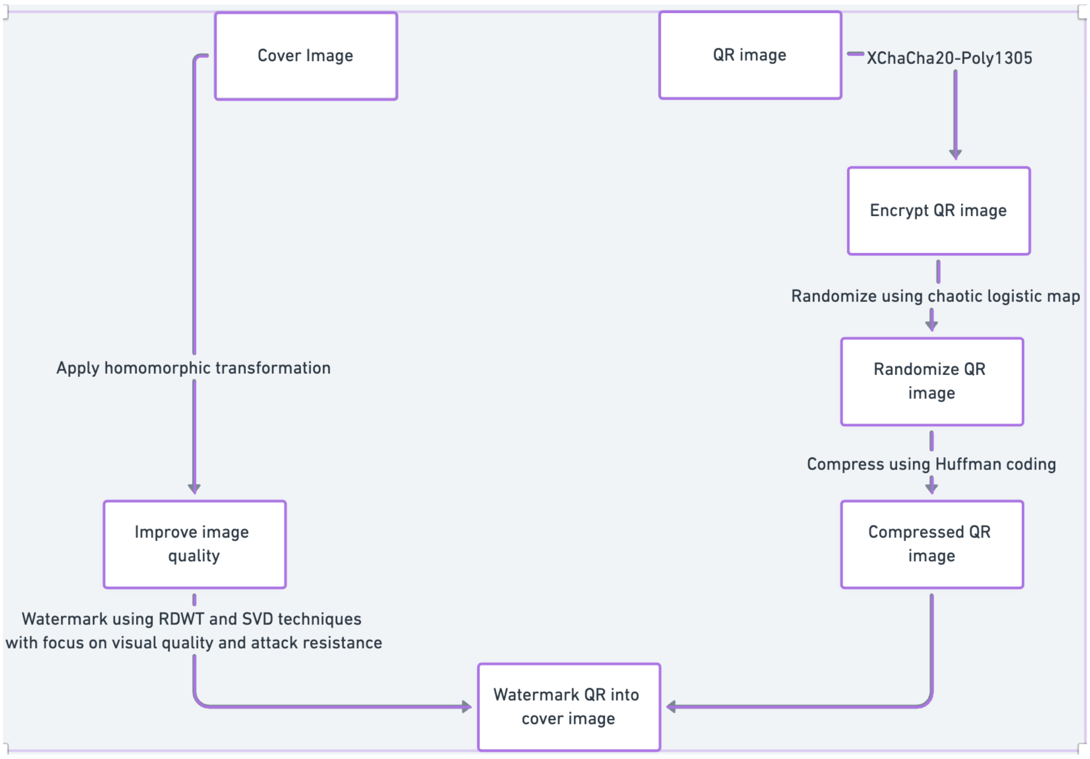
Cover Image
QR image
XChaCha20-Poly1305
Encrypt QR image
Randomize using chaotic logistic map
Randomize QR image
Apply homomorphic transformation
Compress using Huffman coding
Improve image quality
Compressed QR image
Watermark using RDWT and SVD techniques with focus on visual quality and attack resistance
Watermark QR into cover image

Figure 1: Overview of proposed methodology

and an original image. A higher value of PSNR denotes that the watermarked image is less visible from the cover image. It is calculated using the following formula [4]:

$$\boxed{\mathrm{PSNR}(x, y) = 10 \cdot \log_{10} \left(\frac{\max(\max(x), \max(y))^2}{\mathrm{MSE}(x, y)} \right)}$$

where max denotes the image's maximum potential pixel value.

- **Mean Squared Error (MSE)**

The average squared difference between the original and watermarked photos is quantified by the Mean Squared Error (MSE). It is calculated as follows: It is computed as 4

$$\boxed{\mathrm{MSE} = \frac{1}{N} \sum_{i=1}^{N} (I(i) - K(i))^2}$$

where k(i) and k(i) are the pixel values of the original and watermarked images at location i, and N is the total number of pixels.

- **Structural Similarity Index (SSIM)**

The structural similarity between the extracted and original watermark data is evaluated using the Structural Similarity Index (SSIM). The SSIM value scale goes from -1 to 1, with 1 denoting an ideal match [5].

$$\boxed{\mathrm{SSIM}(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}}$$

Where, μ denotes average of variable,σ denotes standard deviation and C_1, C_2 are constants

[4] https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio

[5] https://en.wikipedia.org/wiki/Structural_similarity

3.2.2 Robustness evaluation

Robustness is the watermarked image's capacity to cope with diverse attacks and circumstances while retaining its security and integrity. This approach will make sure that the embedded data can still be found and extracted even after the watermarked image has undergone standard image processing operations like noise addition (Gaussian, Salt & pepper), compression, filtering, or other image alterations. One quantitative indicator that can assess robustness is the Normalized Cross-Correlation (NCC) Shukla and Singh [2023]. The similarity between the two images is higher when the NCC values are closer to 1. A high NCC indicates more resistance to specific kinds of attacks or distortions for the watermark. When it comes to watermarking, a low NCC could indicate that the watermark was severely impacted or destroyed during the application of attacks.

NCC can be calculated as [6]

$$\boxed{\mathrm{NCC}(X,Y) = \frac{\sum_{i=1}^{n}(X_i-\bar{X})(Y_i-\bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i-\bar{X})^2 \sum_{i=1}^{n}(Y_i-\bar{Y})^2}}}$$

Where X and Y are compared images, X_i and Y_i are intensity values at i, $\bar{X}$ and $\bar{Y}$ are means, n is the sample size.

3.2.3 Ownership authentication

In the proposed approach, ownership authentication is evaluated to identify and validate the legitimate owner of the cover image file. This authentication can be achieved by extracting QR watermark data from the cover image, which provides information that uniquely identifies the owner or source.

4 Design Specification

The Design of a proposed architecture involves techniques such as homomorphic transformation of the cover image, XChaCha20-Poly1305 encryption algorithm, chaotic logistic map, and Huffman coding on the QR image. The following section will discuss it in detail.

4.1 Algorithm Functionality

The initial point of the suggested approach is the original high-resolution image. It goes through the following functional components.

- **Homomorphic trasformation:**

This method, which is cited in Zaheeruddin and Suganthi [2019], is used to improve the illumination and contrast of an original image. It involves processing the image using a homomorphic transform module, which first uses the Fourier transform to convert the image from the spatial domain to the frequency domain. Next, a logarithmic operation is carried out, high pass filtering is applied, and finally, the image is converted back to its original form in the spatial domain using the Inverse Fourier transform, but with enhanced features. The overall processing is featured in the Figure 2

[6] https://xcdskd.readthedocs.io/en/latest/cross_correlation/cross_correlation_coefficient.html

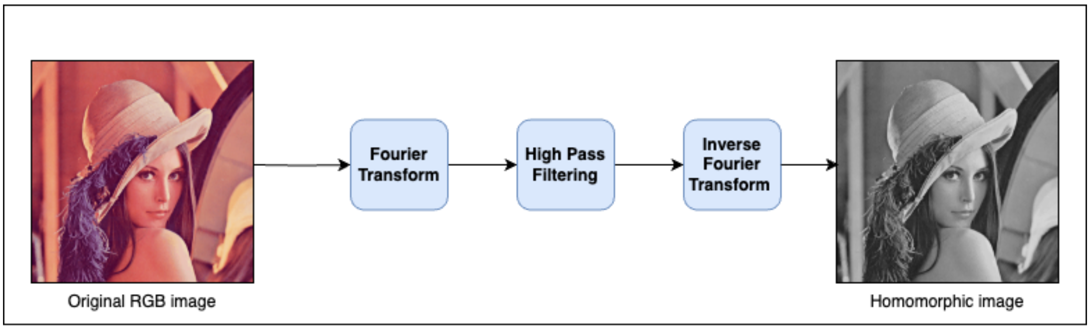

Figure 2: Processing of Homomorphic transformation

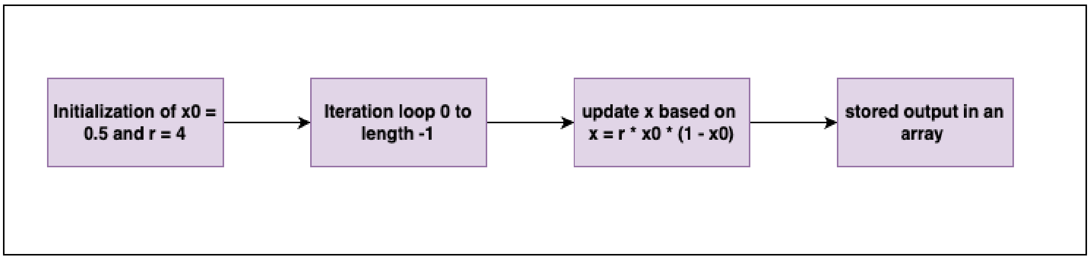
Initialization of x0 = 0.5 and r = 4
Iteration loop 0 to length -1
update x based on x = r * x0 * (1 - x0)
stored output in an array

Figure 3: Working of Chaotic logistic map

- **XChaCha20-Poly1305 Encryption**

In the proposed method, the XChaCha20-Poly1305 encryption algorithm Manullang [2020] is used to produce and encrypt a QR code that represents ownership information, providing a high level of security. It is an authenticated encryption with associated data (AEAD) algorithm. It works by taking a random 256-bit key, a 192-bit nonce, and the plain-text QR image as input. The HChaCha20 function is called upon to produce a subkey by supplying it the original key and the first 16 bytes of a 24-byte nonce. This subkey is then utilized as the key for ChaCha20, together with the remaining 8 bytes of the nonce. This combination creates a larger and more secure nonce space by effectively extending the nonce size.[7]

The working of ChaCha20Poly-1305 is explained in reference [8]

- **Chaotic logistic map**

A chaotic logistic map, which introduces an element of randomness to the encrypted data output from XChaCha20Poly-1305 algorithm Patel et al. [2020]. This technique scrambles the encrypted data and provides unpredictability in the generated output. In the suggested system, The sequence of the logistic map is initialized with x0 as 0.5 which acts as an initial parameter to generate chaotic sequence. r is the bifurcation argument that determines the behavior of the map which is set as 4. The logistic map equation is then applied iteratively, updating the current value x and saving the outcome in the array. The computed values are then saved in the array as unsigned 8-bit integers after being converted to integers in the range [0, 255]. The working flow is represented in the Figure 3

[7] https://pycryptodome.readthedocs.io/en/latest/src/cipher/chacha20_poly1305.html

[8] https://en.wikipedia.org/wiki/ChaCha20-Poly1305

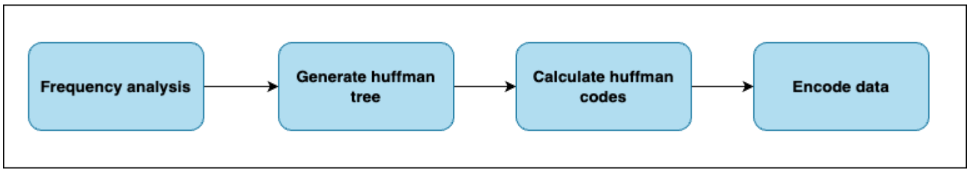

Figure 4: Working of Huffman coding

- **Huffman coding**

Huffman coding [9] in the suggested approach given in the Figure 4 works by noting frequencies, allocates shorter binary codes to more common symbols. Through frequency analysis, a Huffman tree is constructed, with nodes standing in for symbols and their corresponding frequencies. By going through the tree and allocating '0' for left branches and '1' for right branches, Huffman codes are produced. These codes are then used to encode the input data, producing compressed data.

- **RDWT (Redundant Discreet Wavelet Transform) and SVD (Singular Value Decomposition)**

The scrambled and encrypted QR code image is then embedded into the original image using the watermark embedding algorithms RDWT and SVD. RDWT is applied to the original image to obtain different subbands such as LL, LH, HL, and HH subbands of an image at multiple scales. This algorithm produces RDWT coefficients which generate more flexibility while signal processing. Focus is maintained on the LL subband obtained from RDWT and RGB space. SVD is applied on LL to gain U, S, and Vt which are represented as left singular vectors, singular values, and right singular vectors, respectively. Watermark is embedded by modifying singular values. This way encrypted and compressed watermark image gets embedded in the original image. The process elaborated above is shown in Figure 5

Given techniques are integrated to form a hybrid approach of digital watermarking having better performance.

5 Implementation

With an emphasis on the concrete outcomes of the implementation process, the implementation outlines the last phase of the suggested approach.

5.1 Tools and Languages Used

Python programming language and several libraries were utilized in the implementation:

- Python: The main programming language used to construct the watermarking process, which included image processing, QR code generation, and the use of cryptographic tools is Python.
- OpenCV (cv2): It is used for reading, writing, and transforming images due to its broad image processing capabilities.

[9] `https://www.geeksforgeeks.org/huffman-coding-greedy-algo-3/`

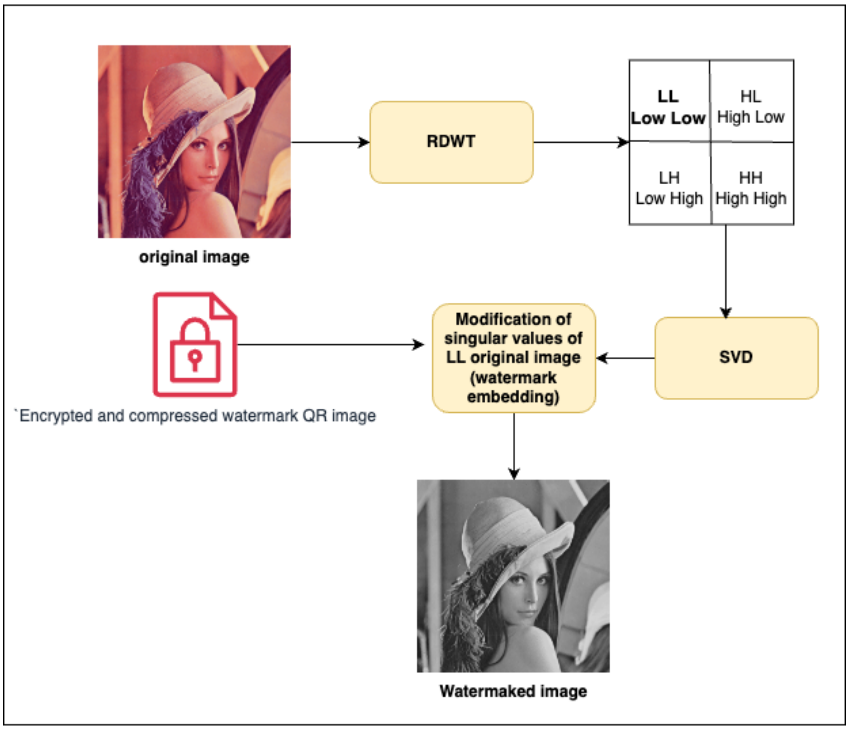
original image
RDWT
LL
Low Low
HL
High Low
LH
Low High
HH
High High
`Encrypted and compressed watermark QR image
Modification of singular values of LL original image (watermark embedding)
SVD
Watermaked image

Figure 5: Image watermarking process

- NumPy: It is used because of its effective array and matrix manipulation, essential for image modification procedures such as SVD.
- SciPy: It offered more scientific computing tools and techniques, such as the SVD function.
- qrcode: A tool for creating QR codes with ownership data embedded in them.
- Cryptography Library: To improve security, the QR codes were encrypted using the XChaCha20Poly1305 module.
- Zlib: It is used to compress the encrypted data to minimize the watermark's visual impact on the image.
- Heapq and Struct: Huffman coding was implemented with the help of these modules, which made for effective data representation.
- PyWavelets (pywt): The Python wavelet transform library is called PyWavelets. It is a component of the image processing pipeline for this project, offering redundant discrete wavelet transform (RDWT) processes that provide multi-resolution analysis.
- scikit-image.metrics: SSIM, MSE, and PSNR: The scikit-image. metrics module contains metrics commonly used to evaluate the quality of images.

5.2 Input and Outputs

The following section describes the inputs provided to the proposed approach and the outputs derived from it.

5.2.1 Inputs provided

- Cover Images: Standard test images are used as explained in section 3
- QR image: QR image is generated from user info using the qrcode library in Python. This picture is used to incorporate as a watermark on the cover image.

5.2.2 Outputs produced

- The main output produced is the cover image watermarked with the QR image that has been compressed, and encrypted.
- The procedure generates several intermediate outputs,
  - The first of which is a gray-scale image that has been illuminated and enhanced with contrast via homomorphic transformation.
  - Whereas, the QR image is encrypted using the XChaChaOPoly-1305 algorithm, resulting in an encrypted image that ensures the robustness of the ownership data.
  - Following that is a chaotic logistic technique in which an encrypted QR image is fed, which scrambles and generates a chaotic sequence of watermark data.
  - Later, the Huffman data compression technique is applied to chaotic sequences, resulting in encoded data streams that ensure the watermark data takes up the least amount of space in the image.

5.3 Implementation Process

The implementation process followed these steps:

- The initial step was to collect significant images to serve as cover images. These images are preprocessed to standardize their size and format.
- Homomorphic filtering is applied to those preprocessed images. The mathematical functions for homomorphic filtering are included in Python's OpenCV (cv2) module. It produces a bright and contrasted image.
- On the other hand, based on the user's information, a QR code image is generated for use as a watermark using the qrcode python package.
- The QR code image is encrypted using the XChaCha20-Poly1305 technique. For encryption, the cryptography.hazmat.primitives.ciphers.aead module's ChaCha20Poly1305 function was used. The ChaCha20-Poly1305 AEAD (Authenticated Encryption with Associated Data) algorithm is implemented in this function, which is part of the cryptography package. ChaCha20-Poly1305 is well-known for its speed and efficacy in transferring secure data. The function uses the ChaCha20 stream cipher for encryption and the Poly1305 authenticator for data integrity verification, resulting in a robust and safe encryption procedure in the watermarking methodology.
- The chaotic logistic mapping applied to the encrypted QR image, which introduces a random factor into the image data, is implemented with mathematical functions and algorithms. NumPy Python package is used to construct chaotic sequences of encrypted QR data.

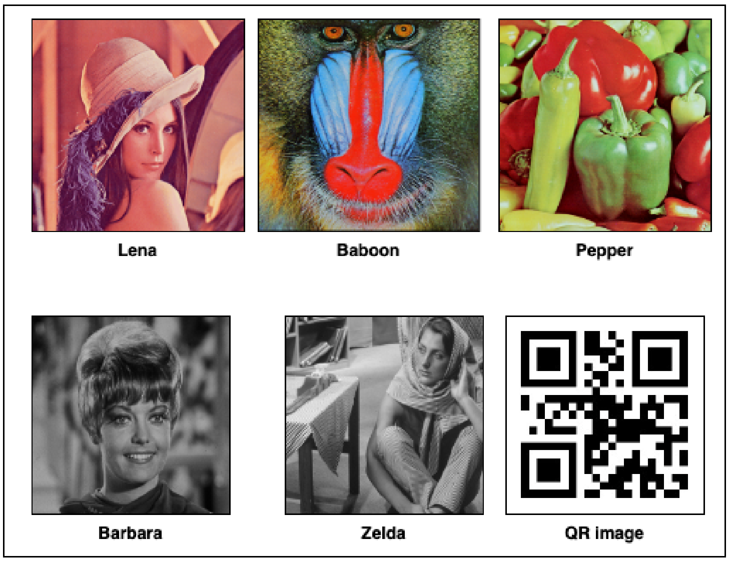

Figure 6: Cover images used and watermark QR image

- The Huffman coding function is used to encode the chaotic sequence of QR picture data. It rendered the use of Python modules such as heapq to manage the priority queue and a dictionary to represent the Huffman tree and numpy for array operations

- As demonstrated in Figure 5, the watermarking process watermarks encrypted and compressed QR images on homomorphically transformed cover images using Python modules like pywt for Redundant Discrete Wavelet Transform (RDWT) and numpy for Singular Value Decomposition (SVD). By making it easier to incorporate watermarking techniques into the image data, these libraries allow the secure and invisible embedding of sensitive data.

6 Evaluation

The proposed hybrid watermarking study is thoroughly reviewed in a critical evaluation using the various evaluation methods indicated in section 3 to determine whether the objectives have been achieved. It is about assessing the system's performance limits and considering design trade-offs.

6.1 Experiment 1 - Imperceptibility analysis

This experiment aims to provide results in terms of watermarked image visual quality, stating the similarity index between the watermarked image and the original image. It is calculated by metrics such as PSNR, MSE, and SSIM. The suggested method's effectiveness is assessed using a variety of color test photos, including Lena, Baboon, Barbara, Pepper, and Zelda as given in Figure 6. Both the QR watermark and the color test pictures used as the cover image have dimensions of 512 x 512. MSE, SSIM, and PSNR are the metrics used to calculate the suggested scheme's imperceptibility.

The experiment is carried out in the programming environment where the evaluation metrics mentioned above are calculated manually by using the Python library skimage.

Images	PSNR	MSE	SSIM
Lena	46.48	1.48	0.99
Baboon	44.31	2.4	0.99
Pepper	46.19	1.56	0.99
Barbara	46.51	1.45	0.99
Zelda	46.43	1.47	0.99

Table 2: Evaluation Metrics for imperceptibility

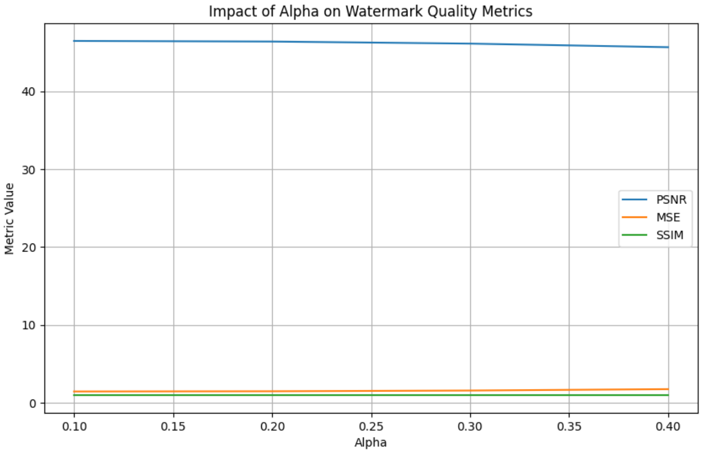

Figure 7: Alpha value impact on evaluation metrics

The outputs are shown in the Table 2 The output indicates the highest PSNR of around 46.51 dB. Higher PSNR (in dB) values indicate less distortion between the two images. The SSIM value of about 0.99 is quite close to one which shows the similarity between original and watermarked images. Lower MSE values suggest a higher degree of similarity between the original and watermarked images, confirming the effectiveness of the imperceptibility goal.

Another experiment on the imperceptibility of watermarked images was conducted to see how visual quality varies when the value of alpha changes. In digital watermarking, the alpha value relates to the intensity of the watermark. Higher alpha values indicate a stronger watermark, but they may produce visual distortions in the watermarked image. Figure 7 depicts the fluctuations in evaluation measures like as PSNR, MSE, and SSIM of alpha values ranging from 0.10 to 0.40. in the case of a watermarked Lena image. It demonstrates a PSNR of 45.66 dB with an alpha value of 0.40, which is less than the achieved PSNR of 46.48 dB with an alpha value of 0.10.

6.2 Experiment 2 - Robustness evaluation

The objective of this experiment is to determine the robustness of a watermarked image. It is calculated by subjecting it to a variety of attacks, including rotation attack, jpeg compression, shift, speckle noise, Gaussian noise, and salt and pepper noise. The NCC of the resulting image and the watermarked image are then compared. Higher NCC values indicate greater robustness, implying that the watermark can withstand the stated attack. Lower NCC values indicate that the attack had a bigger influence on the watermark.

Attacks	NCC - lena	NCC - baboon	Teoh et al. [2023] - lena	Shukla and Singh [2023] - baboon
Gaussian noise	0.99	0.99	0.8993	0.95
Salt & pepper	0.96	0.95	0.96	0.9846
Filtering	0.99	0.91	0.7387	0.97
Speckle noise	0.99	0.99	0.6023	0.86
Shift	0.95	0.85	-	0.98
JPEG compression	0.99	0.97	0.98	-
Rotation attack	0.24	0.27	0.10	-

Table 3: NCC evaluation for robustness

Table 3 denotes the NCC values after each attack between Lena, baboon watermarked images, and post-attack images.

The watermark seems to be quite resilient to JPEG compression and Gaussian noise, somewhat resilient to filtering, shifts, and salt-and-pepper noise, and less resilient to speckle noise and rotational attacks. In most situations, the Lena image appears to be more sturdy than the Baboon image.

6.3 Experiment 3 - Ownership authentication

This experiment aims to confirm the watermarking process by extracting the encoded watermark QR code and reversing all associated algorithms. The processes are carried out in reverse order, and it extracts the watermark that validates the ownership data. Therefore, validation was effective.

For in-depth evaluation, the decrypted QR code can be compared with the original QR code, and check the similarity index between both images. The similarity derived is close to 1 which indicates both images are nearly the same. The evaluation guarantees that the encryption and compression operations are appropriately implemented and that the decryption and decompression processes are reversible, preserving the original data's integrity.

6.4 Discussion

The experiments were structured to test the robustness and imperceptibility of the developed watermarking system across a range of attack scenarios. The choice of high-resolution images for the study was intended to simulate real-world social media usage.

The results obtained are in terms of an average PSNR of 46dB, SSIM of approximately 1, and MSE of 1.67, indicating that the visibility of the watermark QR image in the cover image is lower as per experiment 6.1.

The approach's security is determined by applying attacks such as noise, shift, rotation, filtering, and JPEG compression and calculating it using the NCC metric, which results in around 1 indicating that the watermark will be intact with the cover image in the experiment 6.2. According to Table 3, The results indicate that, in comparison to the Baboon picture, the Lena image generally shows superior resistance to a range of threats. However, depending on the type of attack, different vulnerabilities have different characteristics. Furthermore, the Proposed approach's Lena typically outperforms Teoh et al. [2023] in the majority of situations, particularly when rotation attacks are present and it retains higher image quality metrics.

The experiment 6.3 successfully proves ownership by extracting watermarks. The integrity of the ownership data is ensured by reversing the algorithms. The high similarity index between the original and decrypted QR codes demonstrates that the watermarking procedure is reliable.

The experiments performed in section 6 revealed a good watermarking strategy as per Bull and Zhang [2021]. While the watermark remained largely undetectable, suggesting a successful implementation of the invisibility objective, the robustness against certain types of manipulation needs enhancement. This is a critical point of discussion from previous research, which often prioritized either robustness or imperceptibility. The current design attempted to balance both, yet the findings suggest there is still a trade-off to be addressed. The experiments also uncovered limitations. For instance, while the system performed well under JPEG compression, which is common in social media platforms, it showed vulnerabilities under shift and filtering, indicating a need for improved robustness in these areas.

When compared to existing research, the hybrid approach shows significant improvements in watermark robustness, particularly in its use of chaotic logistic mapping, Huffman coding, and XChaCha20-Poly1305 which were not commonly combined in previous studies. However, these novel integrations also introduced complexity to the system, potentially increasing the computational load and affecting the overall efficiency. The robustness against JPEG compression aligns with findings from Teoh et al. [2023], while the vulnerability to filtering suggests a gap that still exists in watermarking technology, as indicated by Aberna and Agilandeeswari [2023]. The use of chaotic logistic maps for security adds a new dimension to the watermarking discussion, building on the work of Akter et al. [2014] and Mahdieh Ghazvini and Mirzadi [2017], who explored the integration of chaotic systems in encryption.

7 Conclusion and Future Work

The proposed method aimed to research how a hybrid watermarking methodology could improve image ownership protection in the digital world, mainly on social media platforms. The research question centered on the creation and validation of a hybrid system capable of safely and imperceptibly embedding ownership information within digital images using Homomorphic transformation, XChaCha20Poly-1305 encryption, logistic chaotic map, Huffman encoding, and SVD-RDWT digital watermarking techniques. The study was mainly effective in answering the question given, with important findings demonstrating that the hybrid strategy achieved a high level of imperceptibility by maintaining an average PSNR of 46dB and robustness against typical forms of attacks, such as JPEG compression. There are important implications for the digital rights management industry from this research. The study shows how digital assets can be secured using contemporary hybrid watermarking methods, which is essential in the era of social media content sharing. Although the methodology has shown potential in certain scenarios, it has limitations, prominent among them being its resistance to shift and filtering mechanisms. Overall, while the hybrid watermarking method has proven successful in maintaining imperceptibility and improving robustness, there is a significant trade-off that must be balanced.

The suggested watermarking system's future scope spans multiple dimensions, offering greater cross-media applicability by extending its capabilities to new media kinds, such as videos, audio, and animated graphics. Wider attack scenarios could be included in future experiments. A system to notify owners that their assets are being used in an unauthorized way and incorporating machine learning algorithms to predict and counteract potential attacks on the watermark can also be part of the future scope. Real-world testing, particularly on dynamic platforms such as social media, is critical for gaining practical insights into the system's performance and user experience. In terms of commercialization, incorporating the watermarking system into established digital asset management solutions has the possibility of giving artists, photographers, and media corporations a novel tool to protect their intellectual property.

References

P. Aberna and L. Agilandeeswari. Digital image and video watermarking: methodologies, attacks, applications, and future directions. *Multimedia Tools and Applications*, June 2023. ISSN 1573-7721. doi: 10.1007/s11042-023-15806-y.

Mua'ad Abu-Faraj, Abeer Al-Hyari, Charlie Obimbo, Khaled Aldebei, Ismail Altaharwa, Ziad Alqadi, and Orabe Almanaseer. Protecting Digital Images Using Keys Enhanced by 2D Chaotic Logistic Maps. *Cryptography*, 7(2):20, June 2023. ISSN 2410-387X. doi: 10.3390/cryptography7020020. Number: 2 Publisher: Multidisciplinary Digital Publishing Institute.

M. Fatih Adak, Zehra Nur Kose, and Mustafa Akpinar. Dynamic data masking by two-step encryption. In *2023 Innovations in Intelligent Systems and Applications Conference (ASYU)*, pages 1–5, Oct 2023. doi: 10.1109/ASYU58738.2023.10296545.

Afroja Akter, Nur-E-Tajnina, and Muhammad Ahsan Ullah. Digital image watermarking based on dwt-dct: Evaluate for a new embedding algorithm. In *2014 International Conference on Informatics, Electronics Vision (ICIEV)*, pages 1–6, May 2014. doi: 10.1109/ICIEV.2014.6850699.

Sachin Allwadhi, Kamaldeep Joshi, Ashok Kumar Yadav, Rainu Nandal, and Rishabh Jain. A comprehensive survey of state-of-art techniques in digital watermarking. In *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, pages 2362–2368, Dec 2022. doi: 10.1109/ICAC3N56670.2022.10074087.

Sara Alsodairi Abdelhamied A. Ateya Amel Ali Alhussan, Hanaa A. Abdallah. Hybrid watermarking and encryption techniques for securing medical images. *Computer Systems Science and Engineering*, 46(1):403–416, 2023. doi: 10.32604/csse.2023.035048.

Jenan Ayad, Fadhil Sahib Hasan, Alaa H. Ali, Zaid Khudhur Hussein, Hanan J. Abdulkareem, Mustafa A. Jalil, Ghaidaa Ahmed, and Ahmed Sadiq. Image encryption using chaotic techniques: A survey study. In *2021 International Conference in Advances in Power, Signal, and Information Technology (APSIT)*, pages 1–6, Oct 2021. doi: 10.1109/APSIT52773.2021.9641262.

Saharul Alom Barlaskar, Anish Monsley Kirupakaran, Naseem Ahmad, Kuldeep Singh Yadav, Taimoor Khan, and Rabul Hussain Laskar. Imperceptibility and robustness study in different transform domain for copyright protection in digital image watermarking in hybrid svd-domain. In *2023 3rd International conference on Artificial Intelligence and Signal Processing (AISP)*, pages 1–5, March 2023. doi: 10.1109/AISP57993.2023.10135001.

David R. Bull and Fan Zhang. Chapter 4 - Digital picture formats and representations. In David R. Bull and Fan Zhang, editors, *Intelligent Image and Video Compression (Second Edition)*, pages 107–142. Academic Press, Oxford, January 2021. ISBN 978-0-12-820353-8. doi: 10.1016/B978-0-12-820353-8.00013-X.

Reena Devi and Vishal Bharti. Securing image information with lsb steganography technique using matlab tool. In *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, pages 1974–1980, Dec 2022. doi: 10.1109/ICAC3N56670.2022.10074167.

Ranjana Dwivedi and Vinay Kumar Srivastava. An imperceptible and robust image watermarking using rdwt and svd in ycbcr color space. In *2022 IEEE 9th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, pages 1–5, Dec 2022. doi: 10.1109/UPCON56432.2022.9986395.

Zaid Bin Faheem, Abid Ishaq, Furqan Rustam, Isabel de la Torre Díez, Daniel Gavilanes, Manuel Masias Vergara, and Imran Ashraf. Image watermarking using least significant bit and canny edge detection. *Sensors*, 23(3):1210, January 2023. ISSN 1424-8220. doi: 10.3390/s23031210.

T L Kao, H C Wang, and J E Li. Safe mqtt-sn: a lightweight secure encrypted communication in iot. *Journal of Physics: Conference Series*, 2020(1):012044, sep 2021. doi: 10.1088/1742-6596/2020/1/012044.

Antonios Karteris, Georgios Tzanos, Lazaros Papadopoulos, and Dimitrios Soudris. Detection of cyber security threats through social media platforms. In *2023 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, pages 820–823, May 2023. doi: 10.1109/IPDPSW59300.2023.00137.

Priyank Khare and Vinay Kumar Srivastava. A reliable and secure image watermarking algorithm using homomorphic transform in DWT domain. *Multidimensional Systems and Signal Processing*, 32(1):131–160, January 2021. ISSN 1573-0824. doi: 10.1007/s11045-020-00732-1.

Lalan Kumar, Kamred Udham Singh, and Indrajeet Kumar. A compreshensive review on digital image watermarking techniques. In *2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*, pages 737–743, April 2023. doi: 10.1109/CISES58720.2023.10183418.

Samira Lagzian, Mohsen Soryani, and Mahmood Fathy. Robust watermarking scheme based on rdwt-svd: Embedding data in all subbands. In *2011 International Symposium on Artificial Intelligence and Signal Processing (AISP)*, pages 48–52, June 2011. doi: 10.1109/AISP.2011.5960985.

Francisco Lozada-Gonzalez, Manuel Cedillo-Hernandez, and Pedro Guevara-Lopez. Image authentication via zero-watermarking based on a unidimensional cellular automata. In *2023 46th International Conference on Telecommunications and Signal Processing (TSP)*, pages 97–100, July 2023. doi: 10.1109/TSP59544.2023.10197759.

Harshitha M, Ch. Rupa, K. Pujitha Sai, A. Pravallika, and V. Kusuma Sowmya. Secure medical multimedia data using symmetric cipher based chaotic logistic mapping. In

2021 International Conference on System, Computation, Automation and Networking (ICSCAN), pages 1–6, July 2021. doi: 10.1109/ICSCAN53069.2021.9526406.

Breazu Macarie, Morariu Daniel I., Crețulescu Radu G., Pitic Antoniu G., and Bărglăzan Adrian A. In search for the simplest example that proves Huffman coding overperforms Shannon-Fano coding. *International Journal of Advanced Statistics and IT&C for Economics and Life Sciences*, 12(2):3–10, December 2022. doi: 10.2478/ijasitels-2022-00.

Elham Mohamadi Hachrood Mahdieh Ghazvini and Mojdeh Mirzadi. An improved image watermarking method in frequency domain. *Journal of Applied Security Research*, 12 (2):260–275, 2017. doi: 10.1080/19361610.2017.1277878.

Ignatius Timothy Manullang. The Implementation of XChaCha20-Poly1305 in MQTT Protocol. 2020.

Adrian Morales-Ortega and Manuel Cedillo-Hernandez. Ownership authentication and tamper detection in digital images via zero-watermarking. In *2022 45th International Conference on Telecommunications and Signal Processing (TSP)*, pages 122–125, July 2022. doi: 10.1109/TSP55681.2022.9851253.

Seyed Mojtaba Mousavi, Alireza Naghsh, and S. a. R. Abu-Bakar. Watermarking Techniques used in Medical Images: a Survey. *Journal of Digital Imaging*, 27(6):714, December 2014. doi: 10.1007/s10278-014-9700-5. Publisher: Springer.

N.R. Neena Raj and R. Shreelekshmi. A secure pixel level self-recovery scheme for digital images. *J. Intell. Fuzzy Syst.*, 44(3):4481–4493, jan 2023. ISSN 1064-1246. doi: 10.3233/JIFS-221245.

Purba Pal, Sharmila Ghosh, and Nirmalya Kar. Attacks on social media networks and prevention measures. In *2023 International Conference for Advancement in Technology (ICONAT)*, pages 1–6, Jan 2023. doi: 10.1109/ICONAT57137.2023.10080106.

Sakshi Patel, Bharath K. P, and Rajesh Kumar Muthu. Image Encryption Decryption Using Chaotic Logistic Mapping and DNA Encoding, March 2020. arXiv:2003.06616 [cs].

Andy M. Ramos, José A. P. Artiles, Daniel P. B. Chaves, and Cecilio Pimentel. A fragile image watermarking scheme in dwt domain using chaotic sequences and error-correcting codes. *Entropy*, 25(3):508, March 2023. ISSN 1099-4300. doi: 10.3390/e25030508.

Astha Rani, Aditi Purohit, and Rajesh Boghey. Improve secured digital image watermarking with discrete cosine transform and abct. In *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, pages 1761–1767, June 2023. doi: 10.1109/ICCES57224.2023.10192641.

Sakshi Sakshi, Sandeep Verma, Prateek Chaturvedi, and Suman Avdhesh Yadav. Least significant bit steganography for text and image hiding. In *Proceedings of 3rd International Conference on Intelligent Engineering and Management, ICIEM 2022*, Proceedings of 3rd International Conference on Intelligent Engineering and Management, ICIEM 2022, pages 415–421, United States, January 2022. Institute of Electrical and Electronics Engineers. doi: 10.1109/ICIEM54221.2022.9853052. Publisher Copyright:

© 2022 IEEE.; 3rd International Conference on Intelligent Engineering and Management, ICIEM 2022 ; Conference date: 27-04-2022 Through 29-04-2022.

Umme Sara, Morium Akter, and Mohammad Shorif Uddin. Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study. *Journal of Computer and Communications*, 7(3):8–18, March 2019. doi: 10.4236/jcc.2019.73002. Number: 3 Publisher: Scientific Research Publishing.

Dayanand G. Savakar and Anand Ghuli. Robust Invisible Digital Image Watermarking Using Hybrid Scheme. *Arabian Journal for Science and Engineering*, 44(4):3995–4008, April 2019. ISSN 2191-4281. doi: 10.1007/s13369-019-03751-8.

Bipasha Shukla and Kalpana Singh. Based on rdwt and svd arnold transform: A strong and secure image watermarking method. In *2023 International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT)*, pages 265–269, March 2023. doi: 10.1109/DICCT56244.2023.10110042.

Archana Singh, Vinay Kumar Singh, and Shashank Yadav. Image encryption technique using huffman coding and spatial transformation. In *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, pages 352–356, April 2019. doi: 10.1109/ICOEI.2019.8862652.

Tariq Rahim Soomro and Mumtaz Hussain. Social Media-Related Cybercrimes and Techniques for Their Prevention. *Applied Computer Systems*, 24(1):9–17, May 2019. doi: 10.2478/acss-2019-0002.

Liansheng Sui, Han Li, Jie Liu, Zhaolin Xiao, and Ailing Tian. Reversible data hiding in encrypted images based on hybrid prediction and huffman coding. *Symmetry*, 15(6): 1222, June 2023. ISSN 2073-8994. doi: 10.3390/sym15061222.

Yuan Ju Teoh, Huo-Chong Ling, Wei Kitt Wong, and Thomas Anung Basuki. A hybrid svd-based image watermarking scheme utilizing both u and v orthogonal vectors for robustness and imperceptibility. *IEEE Access*, 11:51018–51031, 2023. ISSN 2169-3536. doi: 10.1109/ACCESS.2023.3279028.

A. Vijayalakshmi Venugopal. Copyright concerns of digital images in social media. *The Journal of World Intellectual Property*, 23(3-4):579–597, 2020. ISSN 1747-1796. doi: 10.1111/jwip.12147. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/jwip.12147.

Huanying Wang and Qingtang Su. A color image watermarking method combined qr decomposition and spatial domain. *Multimedia Tools and Applications*, 81(26):37895–37916, 11 2022. Copyright - © The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022; Last updated - 2023-11-30.

Syed Zaheeruddin and K. Suganthi. Image Contrast Enhancement by Homomorphic Filtering based Parametric Fuzzy Transform. *Procedia Computer Science*, 165:166–172, 2019. ISSN 1877-0509. doi: https://doi.org/10.1016/j.procs.2020.01.095.

LLukman Çerkezi and Gökçen Çetinel. Rdwt and svd based secure digital image watermarking using acm. In *2016 24th Signal Processing and Communication Application Conference (SIU)*, pages 149–152, May 2016. doi: 10.1109/SIU.2016.7495699.