A Project Report

on

Digital Watermarking on Multimedia

by

Bhut Tushar, Devesh Parmar

(20BCP023), (20BCP035)

Under the Guidance of

Dr. Payal Chaudhari

Assistant Professor, PDEU

Submitted to

Computer Science and Engineering,

School of Technology,

Pandit Deendayal Energy University

2023

CERTIFICATE

This is to certify that the project report entitled “Digital Watermarking on Multimedia” submitted by Bhut Tushar and Devesh Parmar, has been conducted under the supervision of Dr. Payal Chaudhari, Assistant Professor, PDEU, and is hereby approved for the partial fulfillment of the requirements for the award of the degree of Bachelor of Engineering in the Department of Computer Science and Engineering at Pandit Deendayal Energy University, Gandhinagar. This work is original and has not been submitted to any other institution for the award of any degree.

Sign:

Dr. Payal Chaudhari
Assistant Professor
Computer Science & Engineering
School of Technology
Pandit Deendayal Energy University

Sign:

Dr Rutvij Jhaveri
Assistant Professor
Computer Science & Engineering
School of Technology
Pandit Deendayal Energy University

DECLARATION

We hereby declare that the project report entitled "**Digital Watermarking on Multimedia**" is the result of our own work and has been written by us. This report has not utilized any language model or natural language processing artificial intelligence tools for the creation or generation of content, including the literature survey.

The use of any such artificial intelligence-based tools was strictly confined to the polishing of content, spell checking, and grammar correction after the initial draft of the report was completed. No part of this report has been directly sourced from the output of such tools for the final submission.

This declaration is to affirm that the work presented in this report is genuinely conducted by us and to the best of our knowledge, it is original.

Devesh Parmar & Tushar Bhut
20BCP035 & 20BCP023
Computer Science & Engineering
School of Technology
Pandit Deendayal Energy University
Gandhinagar

Date: 25th November, 2023
Place: Pandit Deendayal Energy University, Gandhinagar

List of Tools Used for the Report with Purpose:

For example,

- **ChatGPT: Correcting Grammar.**
- **Bing AI: Help in writing code for optimizing algorithms.**

ACKNOWLEDGEMENT

We extend our heartfelt gratitude to those whose unwavering support and guidance made the completion of this project possible.

Firstly, we express our sincere appreciation to Dr. Payal Chaudhari for her invaluable guidance, mentorship, and encouragement throughout the development of our project. Her expertise in the field of Cyber Security has been instrumental in shaping our understanding and refining our approach.

We would like to thank our peers and colleagues who provided constructive feedback and engaged in insightful discussions, contributing to the enhancement of our project.

Their collaboration has been a source of inspiration and motivation. Their support has been a pillar of strength, enabling us to navigate challenges with resilience.

Devesh Parmar (Roll No. 20BCP035) and Tushar Bhut (Roll No. 20BCP023)

ABSTRACT

Digital images are easily transferred over the web. Many users use images without the knowledge of their owners. Therefore, a new watermarking system is proposed to ensure copyright protection and image authentication using encryption techniques. Here, a Quick Response (QR) Image containing the public and private keys produced by the cryptosystem is created on the watermarked image. Next, this QR image is encrypted using a chaos logistics map. Public and private keys are used to encrypt and decrypt data. Next, the mixed QR watermark is embedded into the color image using a single-level discrete wavelet transform followed by a singular value decomposition using the key value. Finally, the reverse process is used to remove the watermark. The proposed method is validated using different image processing attacks. The results are then compared with state-of-the-art watermarking systems. Test results show that the system performs well in terms of reliability and theft. Rigorous tests under common image processing attacks demonstrate the technique's reliability and resiliency against unauthorized removal and tampering. Benchmarking against related image watermarking methods proves this system's superior performance for maintaining integrity, recovering watermark data, and thwarting theft attempts. The proposed integration of encryption and QR codes into image watermarking provides a robust solution for asserting image ownership rights.

TABLE OF CONTENTS

List Of Tables

List Of Figures

1. INTRODUCTION

In our rapidly advancing digital era, the importance of safeguarding digital images has become more crucial than ever. The burgeoning growth of the internet has led to an increase in the risks associated with the unauthorized copying and alteration of digital content. This challenge extends beyond the realm of technology; it is about the protection of intellectual property and the preservation of the unique character of digital artworks.

At the forefront of this endeavor is digital watermarking, a technique that is pivotal in the current digital landscape. It is not merely a technical procedure but serves as a vital guardian of intellectual property. This method involves embedding information into images, which, though invisible to the naked eye, provides a strong defense against unauthorized use and piracy. Each digital image is marked with a unique watermark, which acts as a silent but effective protector, ensuring the image is not used without proper authorization. This practice has become a cornerstone in the realm of digital security, offering practical solutions that extend beyond theoretical concepts.

A significant breakthrough in this field is the work of Sanivarapu and colleagues [1]. They have developed an advanced watermarking method that incorporates a Quick Response (QR) code, secured with a dual-key encryption system, into color images. This watermark is designed to be resilient against a variety of image processing attacks, thus maintaining the image's authenticity and legal ownership.

Their approach skillfully uses Discrete Wavelet Transform (DWT), Discrete Cosine Transform(DCT) and Least Significant Bit (LSB), resulting in a watermark that is both strong and imperceptible [1]. This progress marks not only a technological victory but also a significant stride in protecting digital images, merging scientific progress with the safeguarding of creative rights.

Complementing these advancements, the research conducted by Kumar and his team [2] explores the robustness of watermarks, especially against geometric distortions. Their findings contribute to enhancing the security measures for digital images, keeping pace with the continuously evolving online threats.

Digital watermarking thus transcends its role as a mere tool for combating digital piracy. It represents a symbiosis of technology and artistic expression, illustrating a journey through a

changing landscape where innovation in digital security mirrors the persistent resilience and adaptability of the human spirit.

Moreover, the application of digital watermarking is expanding into new and exciting areas, such as metadata embedding, extensively researched by Kamalraj and colleagues [3]. In this aspect, images evolve beyond simple visual objects; they become carriers of extensive information about their origin, context, and journey. The research by Johnson et al. [3] investigates the intricacies of embedding metadata within images, enhancing both their security and their informational value. This approach demonstrates the potential of watermarking to bridge the gap between art and information technology, adding rich layers of meaning and functionality to digital images.

This evolution of digital watermarking signifies a significant step forward in our ability to protect and enhance digital media. It embodies a commitment to advancing technology while respecting and nurturing the creative essence inherent in every digital creation. The ongoing developments in this field underscore the importance of adapting to technological advancements while safeguarding the artistic integrity of digital content.

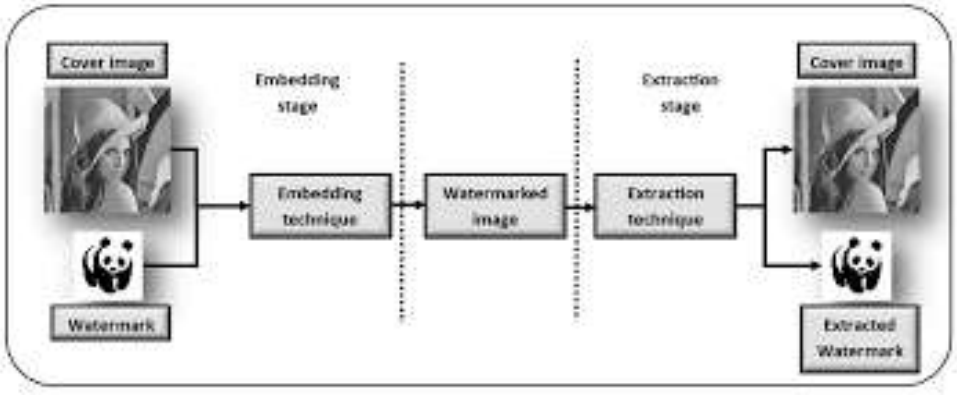

Figure 1 General Overview of Watermarking

2. LITERATURE REVIEW

Hiding information in other media is extremely old based on steganography. The term advanced watermarking first appeared in 1993 when Tirkel et al. [4] presented two methods to hide information in images. Recently, remote healthcare systems have increasingly improved watermarking methods [5]. These approaches provide authentication and security as well as optimal bandwidth utilization, another important criterion for a telehealth communication system. In [5], the authors proposed a watermarking system (WS) for telehealth applications. This method included a signature watermark image and an 80-character patient report using lift wavelet transform (LWT) and discrete cosine transform (DCT) systems.

This work divided the host image into subgroups using LWT, and DCT further transformed the significant subgroups. At the same time, the patient report and signature watermark were encrypted and entered into the final DCT-transformed subsets. An inverse process was used to extract the watermark data. The method offers a combination of watermarking, cryptography and error correction code for electronic patient records (EPR) [6].

Watermark image (WI) and EPR are embedded in this method after performing DWT and turbo coding. Then, an inverse DWT is applied to these embedded data and processed to obtain an encrypted watermark using weaker encryption. At the same time, the cover image is encrypted using a lighter encryption scheme to produce an encrypted cover image. Finally, these encrypted images (overlay and watermark) are re-encoded and sent over the communication channel.

A reverse process is considered in the goal to obtain the desired information. [7] propose a crypto-watermarking system for telemedicine applications. In [7], a blind WS is framed to hide EPR data in a retinal image for telehealth applications. The retinal image is divided into subgroups and the lower subgroup (LL) is subjected to LSB; An EPR watermark is placed on this tape. In the initial stage, bit-level extraction is performed on the host image, and the watermark image is integrated with the host image by the method of chaotic mapping. In addition, the watermarked image (WI) is encrypted using fractional Hartley transforms to obtain a crypto-watermarked image.

Another work [8] is proposed to detect fake medical images using crypto-WS. However, it is a non-blind watermarking system where the EPR is embedded in radiological images for

authentication and security. The approach is based on DCT and compression sensor (CS), where CS is used to encrypt the watermark data and DCT is applied to the host image.

In [9], the authors tried to embed two biometric information of patients, fingerprints and faces, using a two-step watermarking method. Initially, the fingerprint was encrypted using detail extraction and encoding on the original facial image and key. Then, the watermark image was further encrypted and embedded into the original fingerprint to obtain a second level of WI. Finally, the watermark was embedded by combining the DCT sub bands and the encrypted watermark image.

All of the above literature is related to the various fields of image watermarking transformation. They follow different types of watermarking methods based on extraction, and different transformation techniques (most often DWT, DCT, and LWT) are used to embed the watermark. Previous watermarking systems are weak in the security of watermarked data, which inspired us to add cryptographic techniques to protect the watermark.

The proposed watermarking method can overcome authentication problems when embedding a QR code watermark. The proposed model converts text information into a scrambled QR image using a chaotic logistic map. Public and private keys are used to encrypt and decrypt data. Since images are vulnerable to attacks, the proposed method overcomes this using DWT, DCT and LSB using adaptive embedding factor values of images.

The four subgroups of the proposed system, LL, LH, HL and HH, are obtained after one level of LWT. LL is selected based on its effective properties. The LL sub band is decomposed again using the QR code and then to embed the encrypted QR code watermark. The motivation behind this combo is to increase stealth and stamina. Durability is improved by DWT coefficients. The watermark is embedded by changing the DWT coefficients with secret keys. An inverse process is used at the receiver to obtain the watermark data.

Images	PSNR and NCC Values without Attacks		
House	42.25, 1.00	Lake	41.68, 1.00
Tree	43.56, 1.00	Pepper	40.35, 1.00
Girl	42.85, 1.00	House 2	41.74, 1.00
Mandrill	43.12, 1.00	Einstein	43.36, 1.00
Lena	42.22, 1.00	Monalisa	43.81, 1.00
Jetplane	41.81, 1.00	Monarch	42.65, 1.00

Table 1. PSNR and NCC values of earlier developed algorithms

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality. Typical values for the PSNR in lossy image and video compression are between 30 and 50 dB, provided the bit depth is 8 bits, where higher is better. The processing quality of 12-bit images is considered high when the PSNR value is 60 dB or higher.

For 16-bit data typical values for the PSNR are between 60- and 80-dB Acceptable values for wireless transmission quality loss are considered to be about 20 dB to 25 dB in the absence of noise, the two images I and K are identical, and thus the MSE is zero. In this case the PSNR is infinite.

3. METHODOLOGY

This section describes the techniques used in the proposed scheme. The proposed system consists of two modules: loading and unloading. The description of these two processes is given in subsections. Since the transformation domain is stronger than the spatial domain, the DWT algorithm is used in the embedding process because its reconstruction is better without losing information. LSB is used with DWT and DCT to overcome noise and compression attacks. In addition, an encryption algorithm (RSA) is used to ensure that the algorithm is robust against channel vulnerabilities.

3.1. RSA algorithm

RSA is named after the three creators of the RSA calculus, Rivest, Shamir, and Adleman [13]. It is an asymmetric encryption algorithm that contains two keys: public and private. The public key is used for data encryption at the sender and both keys are used for decryption at the receiver. The main reason for the RSA algorithm is that it creates these two keys by multiplying some large integer. Since a public key has two numbers, one of them is a product of two prime numbers. RSA keys are commonly 1024 or 2048 bits in length. If the key's size increases, the encryption's strength increases exponentially. Similarly, using the same prime numbers, a private key is also generated. Therefore, the algorithm's robustness lies in fool proofing the large number factorizing. The RSA algorithm is shown in Figure 1. The public and private keys generated by the RSA algorithm are shown in Table 1.

Figure 2. RSA Algorithm

Inputs and Outputs of RSA Algorithm						
X(o) (0–1)	U (3.56–4)	Prime Numbers	Public Key	Private Key	Encrypted Message	Decrypted Message
0.2	3.6	(3, 5)	(1, 15)	(1, 15)	31514649	(0.2, 3.6)
0.4	3.7	(5, 7)	(23, 35)	(27, 55)	2716334111620	(0.4, 3.7)
0.5	3.6	(5, 13)	(19, 65)	(43, 65)	226273451624	(0.5, 3.6)
0.6	3.8	(5, 11)	(11, 55)	(11, 55)	3746544451461	(0.6, 3.8)
0.8	3.9	(7, 13)	(35, 91)	(35, 91)	55249602528	(0.8, 3.9)

Table 2. Generation of public and private keys using RSA algorithm

The RSA algorithm uses the following procedure to generate public and private keys.

- Choose two large prime numbers r and s.
- Calculate t = r × s by multiplying these values, where t is called the encryption and decryption module.
- Use k less than t so that t is approximately prime to (r − 1) × (s − 1), showing that the only common factor between k and (r − 1) × (s − 1) is 1.
- Choose "k ". " so that 1< k < φ (t), k is a prime φ (t) and gcd (e,d(t)) = 1.
- The public key is <e,t> if t = r × s . Public key <e,t>; encrypt a text message m.
- A mathematical methodology is used to obtain the cipher C of the original message: C = mk mod t. The following formula calculates d and sets the private key so that Dk mod {(r − 1) × (s − 1)} = 1. <d, t> is the private key.
- Private key <d, t> used to decrypt an encrypted text message c. The formula below is used to generate plaintext m from ciphertext c: m = cd mod t.
- Various inputs x(o), u, prime numbers and generated public and private keys with encrypted messages and encrypted messages are shown. in Table 1.

3.2. Discrete Wavelet Transform (DWT)

The main advantage of wavelet analysis over Fourier analysis is its ability to capture time and frequency localization. Daubechies and Mallat introduced DWT in the late 1980s [10,11]. DWT divides the signal into a set of mutually orthogonal wavelet basis functions [10]. 2D-DWT is

commonly used in image processing applications [11]. DWT decomposition of images provides information on low-frequency LL subgroups; horizontal and vertical edge details such as LH and HL sub bands, respectively; and diagonal fringes as HH sub bands. This process is called single-level decomposition, which can be extended to multiple levels to extract new higher-level feature information from images [11]. The decomposition process of the first three levels of the 2D-DWT subgroups is shown in Figure 2. More mathematical details of DWT can be found in [11,12]. The three levels of DWT decomposition are shown in Figure 2, respectively.

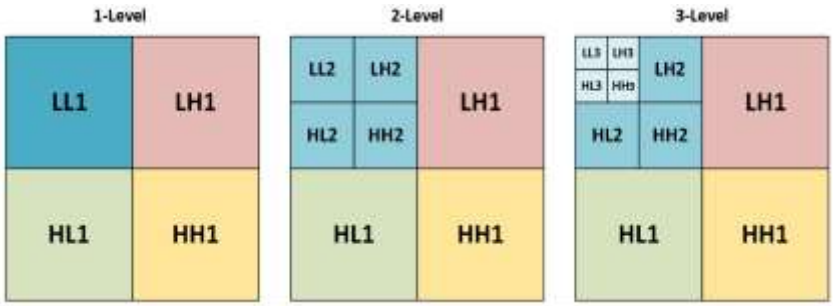

Figure 3. Three levels of DWT decompositions.

3.3. Least Significant Bit (LSB)

The Least Significant Bit (LSB) technique is a widely employed method in image processing, particularly in the context of watermarking [8]. Unlike Singular Value Decomposition (SVD), which involves matrix factorization, LSB operates at the pixel level and is characterized by its simplicity and efficiency.

In the LSB technique, the least significant bit of each pixel in the image is manipulated to embed or encode information, such as a watermark. The advantage of this approach lies in its imperceptibility to the human eye, as a minor alteration in the least significant bit is often visually indistinguishable. The LSB technique can be succinctly expressed with the following formula:

$$I_{\text{watermarked}}(x,y) = \left\lfloor \frac{I_{\text{original}}(x,y)}{2} \right\rfloor \times 2 + \text{bit}_{\text{watermark}}(x,y)$$

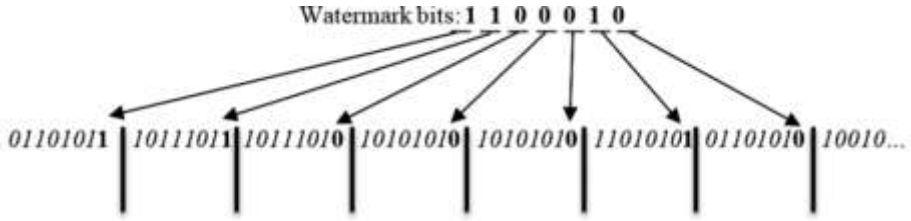

Figure 4. LSB Working

3.4. Discrete Cosine Wavelet

The DCT for Discrete Cosine Transform is a transform associated with the Fourier transform, which is similar to the DFT for Discrete Fourier Transform, but uses only real numbers. The discrete cosine transform is equivalent to a discrete Fourier transform of approximately twice the length. This discrete Fourier transform is performed on a real function, because the Fourier transform of a real function is still a real function, in some variants, it needs to move the input or output position by half a unit. The two-dimensional DCT is taken as an example.

By using the mapping transformation method, the image compression is achieved by transforming each pixel in the image from one space to another, and the signal is transformed from the spatial domain to the frequency domain after DCT. It's a method of orthogonal transformation. It is a special case in the image processing that is widely used in the Fourier transform. The expanded function is a real function, and then discretized, that is a discrete cosine transform. Positive DCT: from spatial domain to frequency domain; inverse DCT: from frequency domain to spatial domain [14].

$$F(u,v) = Af(x,y)\,A^T$$

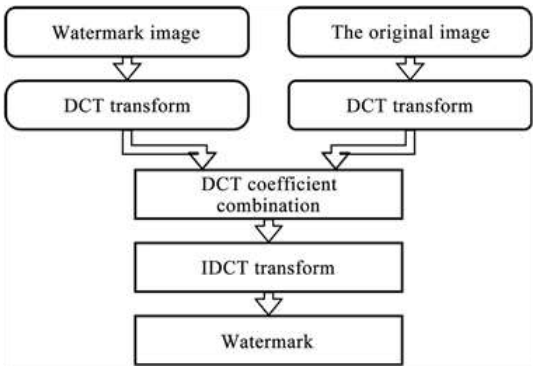

Figure 5. DCT Working

4. PROPOSED METHOD

This section discusses the details of the proposed digital watermarking processes. The proposed system embeds the QR code in the watermark transformation area using DWT and LSB with encryption technique (RSA). The embedding process is described in Section 4.1, and the reverse embedding process was implemented in watermark extraction, which is described in more detail in Section 4.2.

4.1. Embedding

This section covers watermarking using an encryption algorithm step by step. The watermark embedding architecture is shown in Figure 3.

1. Watermark information consisting of encrypted secret message is generated as a QR code.
2. Generate the public key and the encrypted message by entering the private key values into the RSA algorithm.
3. QR code is generated from watermark image and encrypted secret message.
4. The QR code is encrypted using Chaotic Logistic Map (CLM) for watermark security.
5. Import the important image where the watermark should be hidden.
6. Consider the image layer and use DCT to embed the scrambled QR code by modifying the DCT coefficients.
7. Consider the blue layer and use a uniform Haar wavelet distribution to obtain the four subgroups (LL, LH, HL, and HH).
8. As another approach, decompose the blue layer into bit planes and embed the QR code by modifying the LSB plane using LSB substitution.
9. For DCT and DWT, apply inverse transforms to get back the watermarked image layer.
10. A watermarked color image is created by combining a blue layer with red, green and other layers.
11. The watermark image along with the public key and key value is transmitted to the recipient.

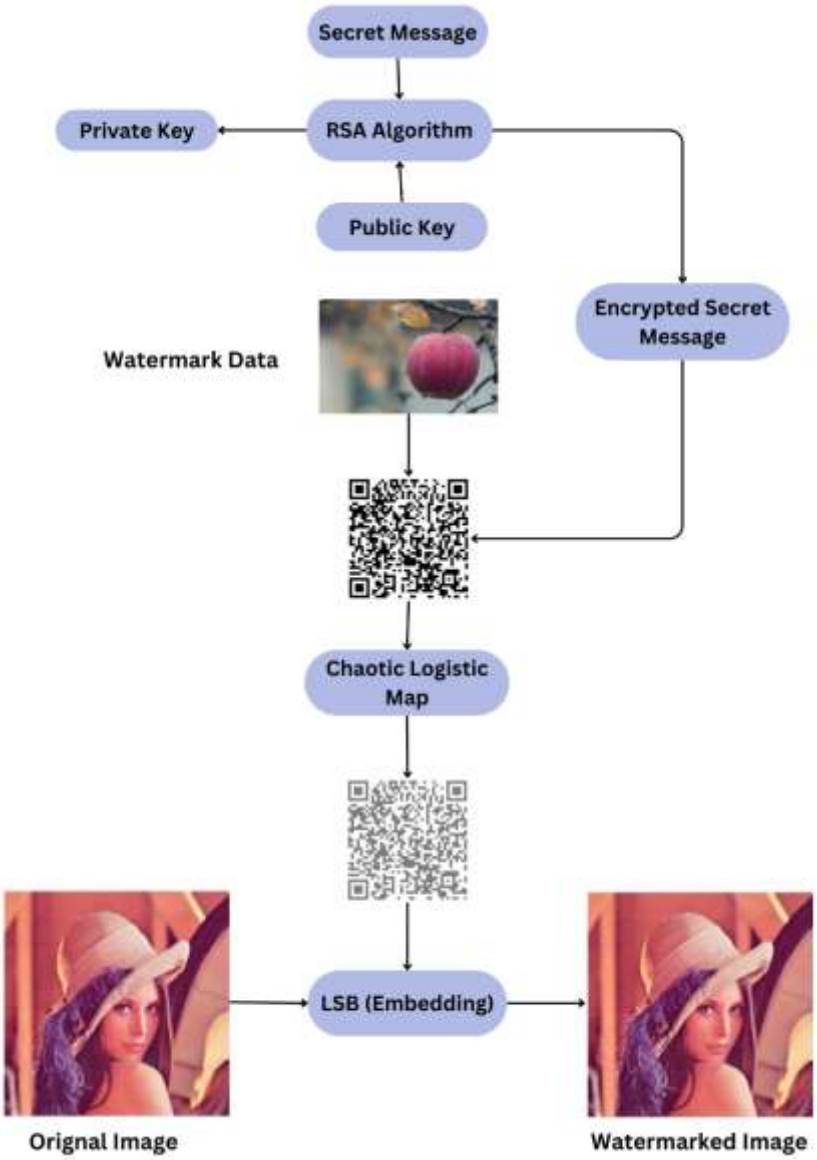

Figure 6. The proposed scheme: embedding process.

4.2. Extraction

This section describes the teardown procedure. Semi-blind watermark extraction requires partial knowledge of important data. The extraction procedure is shown in Figure 5.

1. Display a watermarked image.
2. The color watermark image is converted into different image layers.
3. Since the watermark is embedded in the image component, it is considered to be removed.
4. If DCT is used for embedding:
    - Apply DCT on the blue layer
    - Extract the scrambled QR code watermark by reading the modifications in DCT coefficients
5. If DCT is used for embedding:
    - Apply DCT on the image layer
    - Extract the scrambled QR code watermark by reading the modifications in DCT coefficients
6. If LSB substitution is used:
    - Decompose the blue layer into bit planes
    - Extract the embedded watermark from the LSB plane
7. Apply inverse chaotic encryption using CLM algorithm and private key on the extracted QR code to decrypt it.
8. Decode the QR code to get the watermark information
9. Use RSA public key and private key values to decrypt the watermark message and verify the watermark information.

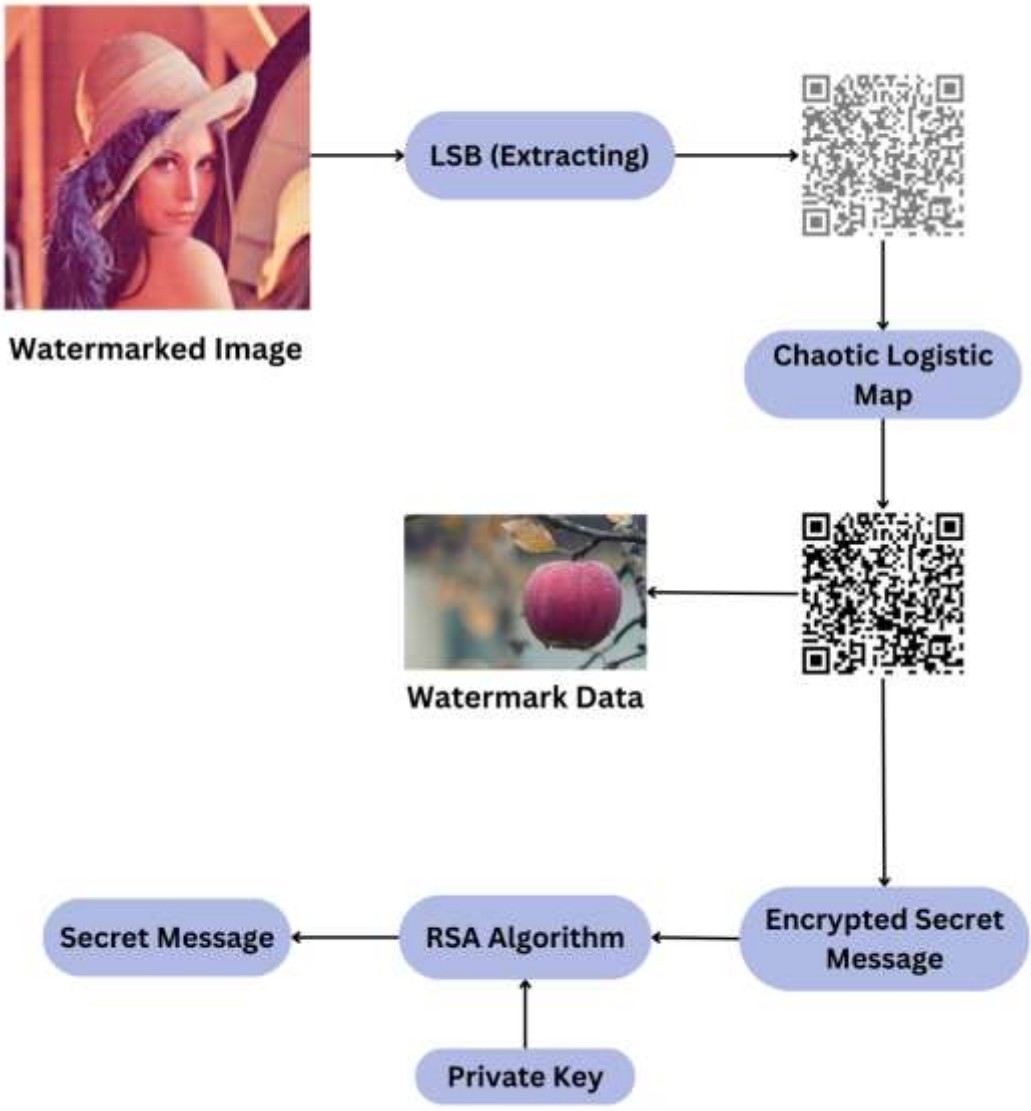

Figure 7. The proposed scheme: extraction process.

5. RESULTS AND ANALYSIS

In the results, sample color images with a size of 100×100×3 and watermark are considered for the evaluation of the proposed method, which is shown in Figure 6 and Figure 7. Several attacks such as noise attacks and geometric attacks are applied to the sample images to test the method's robustness, which is discussed in detail.

Figure 8. The proposed method embedding and extracting

5.1. Evaluation Metrics

The peak-signal-to-noise ratio (PSNR) and normalized correlation coefficient (NCC) metrics evaluate how effectively the proposed watermarking system works. These are discussed in detail in this section.

5.1.1. Peak-Signal-to-Noise Ratio

PSNR is an articulation of the proportion between a signal's most extreme conceivable worth and the watermarked signal. The PSNR is normally represented in the logarithmic decibel scale. PSNR between the watermarked picture and cover picture is utilized to assess intangibility and is effortlessly characterized through the mean square error (MSE).

MSE permits the analysis of the valid pixel upsides of a unique image to a corrupted image. The higher the PSNR values, the higher the quality of the watermarked image:

$$MSE = \frac{\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}(I_{m,n} - WMI_{m,n})^2}{I_{m,n}}$$

$$PSNR_{I,WMI} = 20log_{10}\left(\frac{max_I}{\sqrt{MSE}}\right)$$

The $MAXML$ refers to the extreme value of the image that is possible.

On testing out the algorithm **PSNR value of 28.34** was obtained.

5.1.2. Normalized Correlation Coefficient

NCC is a measure to find the correlation coefficient between the original watermark and the extracted watermark. When NCC is close to 1, the extracted watermark is similar to the original watermark. NCC is defined as:

$$NCC_{qr,eqr} = \frac{\sum_{x=1}^{m}\sum_{y=1}^{n} qr(x,y) \times Eqr(x,y)}{\left(\sqrt{\sum_{x=1}^{m} qr(x,y)^2}\right)\left(\sqrt{\sum_{x=1}^{m} Eqr(x,y)^2}\right)}$$

On testing out the algorithm **NCC value of 29.86** was obtained.

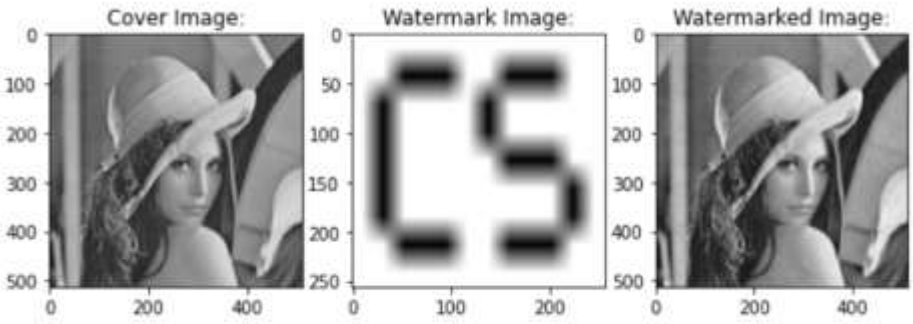

Figure 9. The proposed method output

6. CONCLUSION

In conclusion, our new watermarking technique advances the fields of copyright protection and image authentication by intelligently combining descriptive and spatial domain techniques. Combining the RSA asymmetric cryptographic algorithm with the DWT, DCT and LSB algorithms results in a powerful framework that provides not only a verifiable watermark but also a strong barrier to unauthorized use.

Multiple experiments have been conducted through a variety of image and indicator collision attacks that show the improved performance of the proposed watermarking method compared to existing methods. However, we recognize the limitations in the testing phase, where most of the selected image collections are limited. To achieve a broad and comprehensive understanding, our future plans will expand our reviews to include diverse data sets, including the complex domain of medical imaging. We also increased the noise attacks to boost the technique and its strength.

Our commitment is to advance this watermarking technique to unprecedented levels of versatility and effectiveness, and establish it as a cornerstone in the broader image protection and authentication landscape in our region.

7. REFERENCES

[1] Sanivarapu, H., et al. (2022). A Novel Digital Watermarking Scheme for Color Images Using QR Images. Appl. Sci., 12(8), 8724.

[2] Vaidya, S. P., Rajesh, K. N. V. P. S., Hosny, K. M., & Fouda, M. M. (2022, August 31). Digital Watermarking System for Copyright Protection and Authentication of Images Using Cryptographic Techniques. Applied Sciences.

[3] Mohanarathinam, A., Kamalraj, S., Prasanna Venkatesan, G.K.D. et al. Digital watermarking techniques for image security: a review. J Ambient Intell Human Comput 11, 3221–3229 (2020).

[4] Van Schyndel, R.G.; Tirkel, A.Z.; Osborne, C.F. A digital watermark. In Proceedings of the IEEE 1st International Conference on Image Processing, Austin, TX, USA, 13–16 November 1994; Volume 2, pp. 86–90. [Google Scholar]

[5] Singh, A.K. Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image. Multimed. Tools Appl. 2019, 78, 30523–30533. [Google Scholar]

[6] Anand, A.; Singh, A.K. Joint watermarking-encryption-ECC for patient record security in wavelet domain. IEEE MultiMedia 2020, 27, 66–75. [Google Scholar]

[7] Kaur, G.; Agarwal, R.; Patidar, V. Crypto-watermarking of images for secure transmission overcloud. J. Inf. Optim. Sci. 2020, 41, 205–216. [Google Scholar]

[8] Borra, S.; Thanki, R. Crypto-watermarking scheme for tamper detection of medical images. Comput. Methods Biomech. Biomed. Eng. Imaging Vis. 2020, 8, 345–355. [Google Scholar]

[9] Lebcir, M.; Awang, S.; Benziane, A. Robust blind watermarking approach against the compression for fingerprint image using 2D-DCT. Multimed. Tools Appl. 2022, 81, 20561–20583. [Google Scholar]

[10] Nason, G.P.; Silverman, B.W. The discrete wavelet transforms in s. J. Comput. Graph. Stat. 1994, 3, 163–191. [Google Scholar]

[11] Van Fleet, P.J. Discrete Wavelet Transformations: An Elementary Approach with Applications; John Wiley & Sons: Hoboken, NJ, USA, 2011. [Google Scholar]

[12] Chang, C.; Girod, B. Direction-adaptive discrete wavelet transforms for image compression. IEEE Trans. Image Process. 2007, 16, 1289–1302. [Google Scholar]

[13] Zhou, X.; Tang, X. Research and implementation of RSA algorithm for encryption and decryption. In Proceedings of the IEEE 2011 6th International Forum on Strategic Technology, Harbin, China, 22–24 August 2011; Volume 2, pp. 1118–1121. [Google Scholar]

[14] Alomoush, W., Khashan, O.A., Alrosan, A. *et al.* Digital image watermarking using discrete cosine transformation based linear modulation. *J Cloud Comp* 12, 96 (2023). https://doi.org/10.1186/s13677-023-00468-w