A Robust Privacy-Preserving Architecture for Image Copyright Authentication based on the Blind Watermarking Approach and Elliptic Curve Cryptography

Crystal Dzebu
West End University College,
Faculty of Computer Studies, Accra
Ghana

Bernard Adjei Buckman
West End University College,
Faculty of Computer Studies, Accra
Ghana

Evans Boye
West End University College,
Faculty of Computer Studies, Accra
Ghana

ABSTRACT

This paper presents an Image Copyright Protection and Authentication System (ICPAS) that performs secure digital watermarking for image identification, authentication, and copyright management. The system introduces a hybrid RGB-YUV transposition blind watermarking approach, combining discrete wavelet transform (DWT), discrete cosine transform (DCT), Arnold transform, and Elliptic Curve Diffie-Hellman (ECDH) key exchange. This method ensures robust watermark embedding and extraction, achieving high imperceptibility and resilience against attacks such as JPEG compression, blurring, cropping, and zoom. Experimental results demonstrate the system's effectiveness, with high peak signal-to-noise ratio (PSNR) and normalized correlation coefficient (NCC) values, validating its ability to protect image integrity and authenticate copyrights. The system architecture is designed for scalability and security, integrating key and license servers to ensure privacy and efficient data handling.

Keywords

Digital Watermarking, Copyright Protection, Image Authentication, Elliptic Curve Diffie-Hellman (ECDH), Discrete Wavelet Transform (DWT), Hybrid Watermarking Scheme

1. INTRODUCTION

The rapid advancements in digital technology have led to a surge in the creation and distribution of digital content [1]. While these advancements have brought numerous benefits, they have also introduced significant challenges related to content protection. The ease of duplication and manipulation of digital content has made it vulnerable to unauthorized access, alteration, and distribution [2].

To address these concerns, digital watermarking has emerged as a promising solution. Watermarking involves embedding imperceptible information, known as a watermark, into digital content. This watermark can be used for various purposes, including copyright protection, content authentication, and tamper detection [2].

Image watermarking, a specific application of digital watermarking, focuses on embedding watermarks into images. The watermark should be invisible to the human eye but robust against common image manipulations such as cropping, resizing, and compression. By embedding a watermark, it becomes possible to verify the authenticity of an image and track its distribution [3].

2. LITERATURE REVIEW

Various types of watermarking systems have been recommended for use in handling different applications.

The author of [4] proposed a watermarking method to protect the integrity and ownership of medical images. The method uses the least significant bit (LSB) technique, which was compared to the dual watermarking (DUALWM) technique. The LSB method was found to be more efficient than DUALWM, as it requires less memory storage and has a shorter execution time.

The author of [2] proposed a fragile watermarking method that embeds image texture into the least significant bit (LSB) of the original host image. The texture features are extracted from the left and right singular matrices of singular value decomposition (SVD). The PSNR of the watermarked image is 51.16dB, which indicates that the watermark is imperceptible.

Priyanka et al. proposed a spatial domain watermarking method in [5] that uses the least significant bit (LSB) technique.

In [6], the authors proposed a watermarking method in the YCoCg-R color space. The embedding step is in the frequency domain, where the DCT is applied to the Y component of the host image. Each bit of the watermark is inserted in three different blocks. The Arnold transform is also used to scramble the Y component and the watermark. The PSNR value is 38.20, and the method is resilient to rotation, salt and pepper noise, and JPEG compression.

The paper [7] proposes a watermarking method that uses the multi-resolution domain and the singular value decomposition (SVD). The original image is first decomposed by the discrete wavelet transform (DWT) into three levels of low frequency sub-bands. The singular values matrix of the third level low frequency sub-band is then extracted for watermarking embedding. The key points are selected by scale-invariant feature transform (SIFT) in the original image and attacked image.

The proposed scheme first encrypts the host image using a symmetric encryption algorithm. Subsequently, the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are applied to the encrypted image to extract the high-frequency coefficients. The watermark is embedded in the high-frequency coefficients using a spread spectrum technique. The watermarked image is then decrypted to obtain the final watermarked image.

3. METHODOLOGY

Figure 1 illustrates the general architecture of the proposed ICPAS system. The proposed ICPAS system has three sub-systems: License Server, Key Server, and Content Server. The License Server generates unique QR codes for image authentication, embedding, extraction, and verification. The Content Server stores verified QR-embedded images and images awaiting verification. The Key Server handles symmetric encryption and decryption key sharing for both the sender and receiver. Each image is assigned two sets of symmetric keys: one for image encryption and another for watermark encryption. To ensure security and prevent interception, the Elliptic Curve Diffie-Hellman Key Exchange protocol [8] is used for key exchange between the Key and License servers.

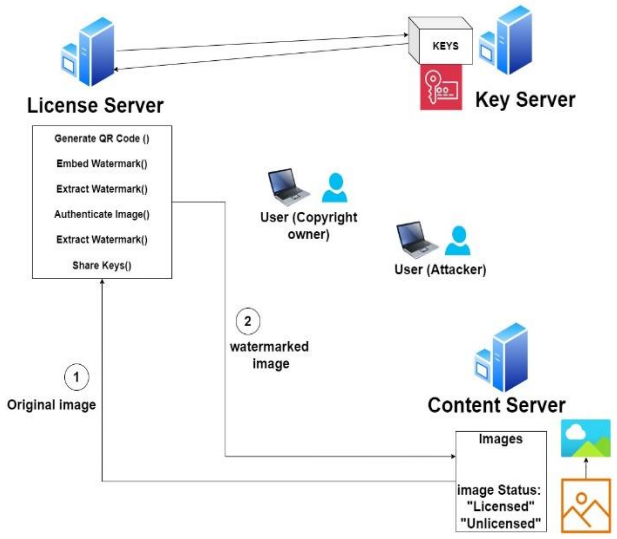

Figure 1: General Architecture of Proposed ICPAS System

3.1 Privacy Preserving Architecture for our ICPAS

Figure 2 shows the proposed architecture for preserving the privacy of key sharing and encryption/decryption processes in the ICPAS system.

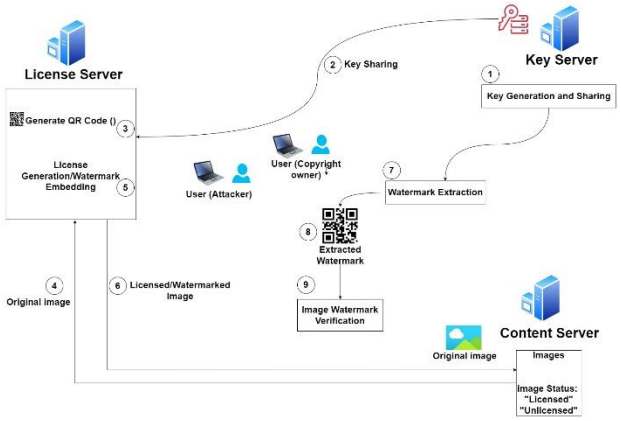

Figure 2: Privacy Preserving Architecture for the proposed ICPAS system

The keys used to embed QR watermarks into the images are encrypted using ECDH Key exchange protocol and stored on the Key server. This encrypted key can then be decrypted on the License Server and used to embed and extract the image QR watermarks. This prevents attackers from eavesdropping and compromising the key, thus ensuring a secure system.

The proposed watermarking scheme leverages the concepts of RGB to YUV Transformation, Discrete Wavelet Transform (DWT), Discrete Cosine Transformation (DCT), and Arnold Transform. These concepts are discussed one by one in the next section.

3.2 Transforming from RGB to YUV color space

The YUV color space is a color space that is often used in image processing and video encoding. It is a perceptually uniform color space, meaning that the human eye is more sensitive to changes in luminance (Y) than in chrominance (U and V). This makes the YUV color space well-suited for applications where it is important to preserve the quality of the image, such as video compression. We adopt this transformation in our paper as follows [9]:

$$Y = 0.299 * R + 0.587 * G + 0.114 * B \quad (1)$$

$$U = -0.147 * R - 0.289 * G + 0.436 * B \quad (2)$$

$$V = 0.615 * R - 0.515 * G - 0.100 * B \quad (3)$$

To transform from YUV back to RGB colour space, the following equations are used:

$$R = Y + 1.144(v - 128) \quad (4)$$

$$G = Y - 0.392(U - 128) - 0.813(V - 128) \quad (5)$$

$$B = Y + 2.017(U - 128) \quad (6)$$

where R, G, and B are the Red, Green and Blue components of each pixel, and Y, U, and V are the YUV components of each pixel.

3.3 Discrete Wavelet Transform (DWT)

The Discrete Wavelet Transform (DWT) provides multi-resolution image representation and flawless reconstruction of

deconstructed images. A discrete wavelet is expressed as:

$$\psi_{j,k}(t) = a_0^{-\frac{j}{2}}\psi(a_0^{-j_t} - kb_0) \quad (7)$$

Dyadic wavelets are a type of wavelet that are based on a dyadic scale, meaning that they are scaled by powers of 2. This makes them well-suited for applications where the signal is sampled at regular intervals, such as digital images.

In this research, dyadic wavelets where $a_0 = 2$ and $b_0 = 1$ were employed by substituting these values into equation (7) as follows:

$$\psi_{j,k}(t) = 2^{-\frac{j}{2}}\psi(2^{-j_t} - k) \quad (8)$$

When an image is processed through low and high pass filters, DWT decomposes it into sub-bands with different resolutions. This paper uses a two-level Haar wavelet, a dyadic wavelet with two resolution levels [10].

3.4 Discrete Cosine Transform

The Discrete Cosine Transform (DCT) is a mathematical operation that transforms an image from the spatial domain to the frequency domain. The spatial domain is the domain of the original image, where each pixel is represented by its intensity value. The frequency domain is the domain of the transformed image, where each pixel is represented by its frequency components. The DCT transform can be used to embed a watermark into an image in a way that is both imperceptible and robust to attacks. The watermark is embedded in the frequency domain of the image, where it is less likely to be detected or removed.

Given an original image, $f(x, y)$, the DCT is defined by:

$$F(u,v) = c(u)c(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times cos\frac{\pi u(2x+1)}{2M} cos\frac{\pi v(2y+1)}{2N} \quad (9)$$

Where M and N are rows and columns respectively and $c(u)$ and $c(v)$ are given by:

$$c(u), c(v) = \begin{cases} \frac{1}{\sqrt{2}}, & if\ u, v = 0 \\ x, & otherwise \end{cases} \quad (10)$$

The inverse DCT is used to transform the image from the frequency domain back to the spatial domain and is given as:

$$f(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} c(u) \times c(v)F(u,v) \times cos\left[\frac{\pi}{M}u\left(x+\frac{1}{2}\right)\right] cos\left[\frac{\pi}{N}v\left(y+\frac{1}{2}\right)\right] \quad (11)$$

3.5 Arnold Transform

The proposed system employs the Arnold Transform to enhance the security of the images. The Arnold transform is a mathematical operation that scrambles the pixels of an image in a chaotic way. The Arnold transform is periodic, meaning that after a certain number of iterations, the image will return to its original state. This property of the Arnold transform is used in image watermarking to make it more difficult to remove the watermark. The Arnold transform is given by the following formula:

$$x' = ax + bmodm \quad (12)$$

$$y' = ay + bmodm \quad (13)$$

Where x and y are the original coordinates of a pixel, a and b are random numbers, and m is the size of the image. The watermark is embedded in the chaotic scrambled image, making it difficult to detect or remove [11].

3.6 Singular Value Decomposition (SVD)

In watermarking, SVD can be used to embed a watermark into an image by modifying the singular values of the image matrix. The watermark data is typically embedded in the lower-order singular values, as these are less perceptually important than the higher-order singular values.

To extract the watermark from the watermarked image, the SVD of the image matrix is calculated. The watermark data can then be recovered by extracting the lower-order singular values from the SVD decomposition.

Singular value decomposition (SVD) is a mathematical technique that can be used to decompose a matrix into three component matrices; That is: A diagonal matrix of singular values S, a matrix of left singular vectors, U and A matrix of right singular vectors, V.

Given a rectangular matrix A, of size mxn, the SVD of matrix A can be expressed as:

$$A_{mn} = U_{mm}S_{mm}V_{nn}^T \quad (14)$$

Where

$$S = \begin{bmatrix} \lambda_1 & 0 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 & 0 \\ 0 & 0 & ... & 0 & 0 \\ 0 & 0 & 0 & ... & 0 \\ 0 & 0 & 0 & 0 & \lambda_m \end{bmatrix} \quad (15)$$

where S is a diagonal matrix that contains the square roots of eigenvalues, $\lambda_1, \lambda_2, \lambda_3, \ldots \lambda_m$ from matrix U to Matrix V in a descending order.

Note that $U^TU = I$ and $V^TV = I$ where the columns of matrix U are orthonormal eigenvectors of A^TA and the columns of the matrix V are orthogonal eigenvectors of matrix A^TA.

3.7 The Watermarking Algorithm

Image watermarking can be divided into two categories: blind and non-blind. Blind watermarking does not require the original image or any other information to extract the watermark. Non-blind watermarking requires the original image to extract the watermark.

Blind watermarking is the most prevalent approach in practical applications because the original image is not always accessible during the watermark extraction stage. For example, if an image is watermarked and then distributed online, the original image may not be available to the person who wants to extract the watermark. In this paper, we propose a Hybrid RGB Blind Watermark scheme which combines the DWT (2-Level Haar Wavelet Transform) with DCT and Arnold and ECDH Key exchange.

The proposed watermarking algorithm involves two main steps: watermark embedding and watermark extraction. The RGB input image is transformed into YUV space before embedding and vice versa after extraction. A unique watermark QR-Image is generated and inserted into the image. During the insertion process, the original image is first converted by n-level DWT.

Algorithm 1: Watermark Embedding Algorithm

Input: Input image with size: mxn.

Output: Image with embedded watermark.

1: Read Cover Image of mxn size, separate it's R,G,B components and transform into YUV color space using equations (1), (2) and (3).

2: Transform the host image into a two-dimensional discrete ripple (2DDWT) domain to obtain four distinct sets of multi-resolution coefficients (LL_1, HL_1, LH_1 *and* HH_1).

3: Convert the HL_1 sub band to the DWT domain to make 4 smaller sub bands and select HL_2 and LH_2.

4: Select U component and Apply 2-Level DWT to HL2 and LH2 sub bands.

5: Read grey scale QR watermark image of size mxn and reconstruct it a vector consisting of 0s and 1s.

6: Using the key generated and shared by ECDH Key exchange, generate two PN sequences for a given watermark that are the same size as HL_2 and LH_2.

7: Make sure it is 1 for each pixel of the watermark and if it is 0 without changing HL_2 and LH_2, add HL_2 and LH_2 by multiplying these PN sequences by the argument K, where K is the gain factor according to the equation:

$$X' = X + K \times pn_{sequence} \quad (16)$$

8: Compute a Summation of all elements in the pn sequence with the function SUM() .

9: Find Arnold Periodicity P for the given watermark.

10: Use a function CheckSum() to check whether SUM returned in Step 6 , SUM>T, where T is a predefined threshold value. If SUM>T, perform Arnold Watermark Scrambling by using the Key, K2=P+ count, otherwise use the equation K3=P-count to perform the Arnold Watermark Scrambling, where count is the predefined counter value.

11: Generate two pseudorandom number (pn) sequences: pn_sequence_0 and pn_sequence_1, based on the sum of all mid band elements needed for 4x4 DCT transformation.

12: Embed the watermark using the following equations:

If QR-Watermark bit = 0, then

$$P' = P + K \times pn\_sequence\_0 \quad (17)$$

If QR-Watermark bit=1, then

$$P' = P + K \times pn\_sequence\_1 \quad (18)$$

Where P is a matrix of DCT Transformed block's mid band coefficients and P' is the Watermarked DCT block.

13: Apply Inverse Discrete Cosine Transform to get "New*HL2"* and "New*LH2" respectively.*

14: Apply Inverse Discrete Wavelet Transform with "LL1, New*HL2, NewLH2, LH1, HH1" to get "New_U" component.*

15: Combine Y, New_U and Q components and convert to RGB color space using equation

(4), (5), (6).

Algorithm 2: Watermark Embedding Algorithm

Input: Image with embedded watermark of size: mxn.

Output: Final watermark.

1: Read Watermarked Image of mxn size, separate it's R,G,B components and transform into YUV color space using equations (1), (2) and (3).

2: Select U component and Apply 2-Level DWT to HL2 and LH2 sub bands.

3: To generate two pseudorandom number sequences (pn_sequence_0 and pn_sequence_1), divide the DCT blocks into 4x4 sizes, and use the sum of the mid band elements to determine the sequences. The same seed from the watermark embedding process must be used.

4: To extract mid band elements from a DCT block, divide the block into 4x4 subblocks, calculate the mid band coefficients, and find the correlation between these coefficients and the two PN sequences, pn_sequence_0 and pn_sequence_1.

5: To determine watermark bits, compare the correlation coefficients between the extracted mid band coefficients and each PN sequence. If pn_sequence_0's coefficient is higher, record the bit as 0; otherwise, record it as 1. These bits are used to recreate the intermediate watermark.

6: To obtain the final recovered watermark, the intermediate watermark is scrambled using the Arnold scrambling algorithm.

3.8 Implementation of Elliptic Curve Diffie-Hellman (ECDH) algorithm for Encoding Keys

The Elliptic Curve Diffie-Hellman key exchange is a cryptographic protocol that uses elliptic curve cryptography to securely generate a shared secret key between two parties over an insecure communication channel.

The algorithm for calculating symmetric keys is much simpler and more efficient from a computational point of view when using Elliptic Diffie-Hellman curves [12], [13]. First, Bob and Alice accept the prime and integer parameters a and b of the equation of the elliptic curve $y^2 = x^3 + ax + b\ (mod\ p)$ and a base argument $G\ (x,\ y)$ carefully chosen in the elliptical group when increasing operation. The generation of domain parameters is not implemented by either transmitter or receiver because it requires calculating the number of arguments on the curve which are long and difficult to implement. Domain of the parameters of the elliptical curve Fp is well-defined as the equation $T\ (p,\ a,\ b,\ G,\ h)$, where p is field that the curve is defined over, $a,\ b$ he elliptic curve equation coefficient, G the generator point is the group building elements, n is prime directive of G i.e. optimistic integers lowest is nG = 0, and h cofactor, quantity of end in the group elliptic $E_p\ (a,\ b)$ divided by n.

The proposed system leverages the Elliptic Curve Diffie-Hellman (ECDH) Key Exchange algorithm [14] to ensure privacy of key exchange between the License and Key Server.

To ensure a robust key exchange between the Key server, License server and client server, the ECDH algorithm which requires a message mapping table to be an argument on the elliptical curve was used

The elliptic curve with equation $y^2 = x^3 - 4mod257$ was simulated, where a=0 and b = -4 was used to generate an elliptic curve argument from an algebraic calculation.

To be able to generate (x, y) curve points, the elements of the top elliptic curve, which are: $F_{257}\ \{0,1,2,3,\ldots 256\}$ were first determined. The Quadratic Residue Module to determine the elements of an elliptical curve group are a set of resolutions from $y^2 = x^3 - 4\ mod\ 257\ for\ x, y \in F_{257}$ was then computed,

The elements inside F_{257} were calculated to determine all points in the elliptic curve. For example $(x_1, y_1) = (2,1)\ and\ (x_1, y_1) = (8,3,7)$, then P + Q can be calculated. The outcomes of the accumulation and multiplication procedures of all note into arguments located in the elliptic curve are then computed and visualized.

3.9 Experimental Setup

To demonstrate the simulation, two sample images referred to as Image 1 and Image 2 (see Figure 3), were captured and embedded with unique QR codes. Subsequently, eight attacks, including JPEG compression, median filtering, custom blur, watermarking, Gaussian blur, salt and pepper noise, horizontal cropping, vertical cropping, and zoom attacks, were executed on these watermarked images to assess the robustness and security of the proposed watermark extraction algorithm.

All the images used have no copyright issues and were captured by the researchers for the purpose of the experiment.

To verify the watermark in a potentially attacked image, it is crucial that the extracted watermark is clear and easily recognizable. The robustness of the scheme was assessed by comparing the original watermark with the extracted one using the Normalized Correlation (NC) coefficient, as defined in [15].

PSNR (Peak Signal-to-Noise Ratio) was also used to measure the effectiveness of noise reduction in images. A higher PSNR value indicates better noise reduction and image quality, with the first-captured image as the reference and the attacked image as the comparison [15].

The programming language implemented in python 3.6.12 and Experiments were implemented on a server-based Ubuntu 20.04.6 LTS.. The system was an Intel Core i7 and equipped with four graphic processing units (GPUs) of NVIDIA GeForce RTX 2080Ti with 11 GB memory each.

Image 1 **Image 2**

Figure 3: Cover Image

4. RESULTS FOR PEAK SIGNAL TO NOISE RATIO (PSNR) AND NORMALIZED CORRELATION COEFFICIENT (NCC)

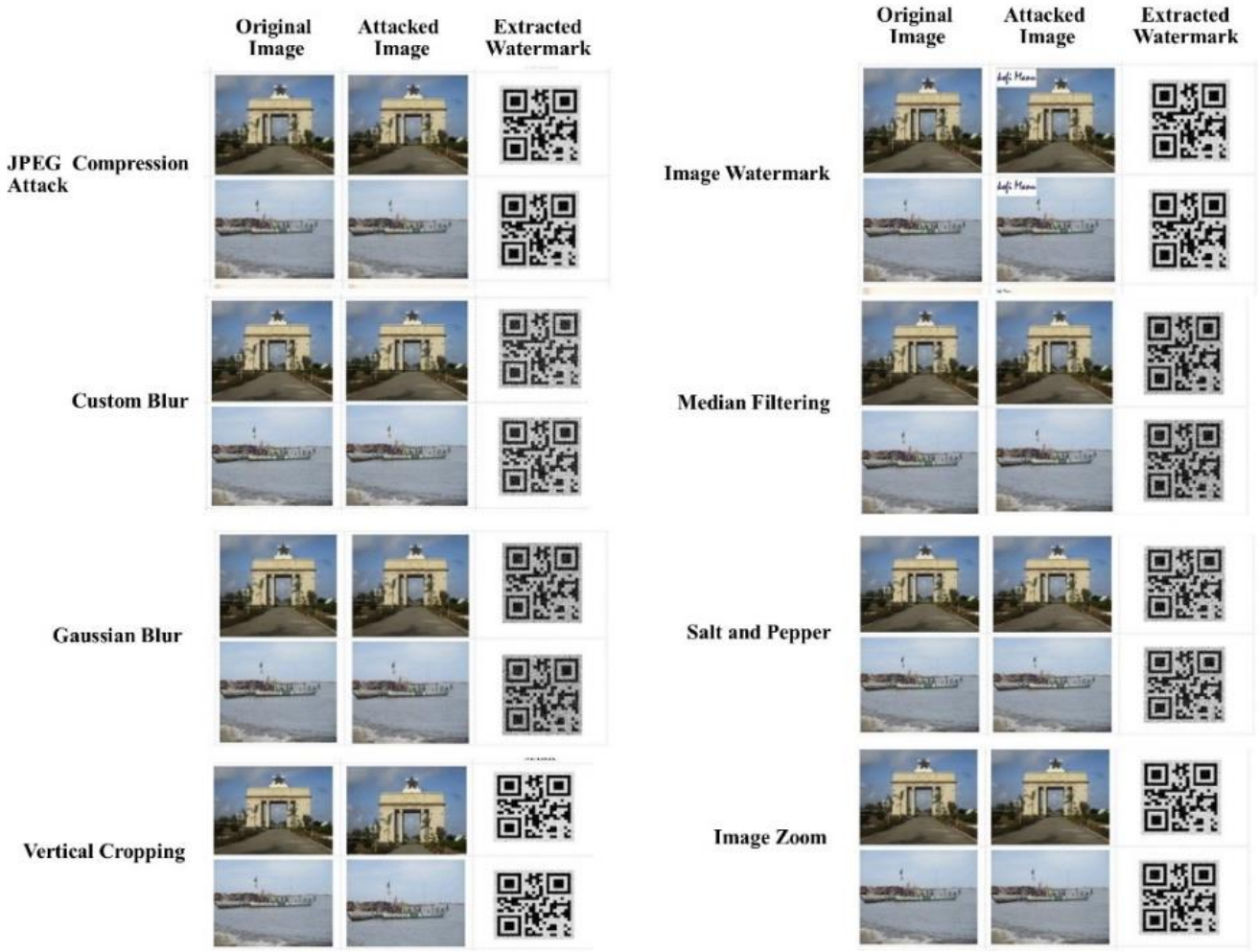

Figure 4: Comparison of Extracted watermarks from Original Cover Image versus Attacked Images

Table 1: Comparison of PSNR and NCC of watermarks against various attacks

Attack	Factor	PSNR (Image 1)			NCC (Image 1)			PSNR (Image 2)			NCC (Image 2)		
		R	G	B	R	G	B	R	G	B	R	G	B
No attack		67.563	67.562	67.565	1.000	1.000	1.000	66.263	66.265	66.261	1.000	1.000	1.000
JPEG Compression	Quality Factor =15%	61.766	61.758	61.764	0.945	0.946	0.944	61.073	61.071	61.069	0.937	0.938	0.938
Custom Blur		58.077	58.072	58.068	0.956	0.955	0.953	58.637	58.636	58.638	0.983	0.985	0.983

Gaussian Blur	K=7	57.638	57.653	57.634	0.966	0.965	0.968	56.917	56.915	56.914	0.935	0.932	0.933
Horizontal Cropping	P=3.5%	51.067	51.078	51.058	0.889	0.887	0.888	51.081	51.084	51.082	0.871	0.871	0.873
Vertical Cropping	P=3.5%	62.376	62.385	62.369	0.950	0.948	0.951	62.116	62.113	62.115	0.949	0.947	0.948
Image Watermark		61.203	61.207	61.211	0.935	0.933	0.934	60.872	60.868	60.873	0.931	0.928	0.929
Median Filtering	(3x3)	58.154	58.161	58.157	0.951	0.953	0.953	57.059	57.055	57.053	0.948	0.948	0.951
Salt and Pepper Noise	P=10%	58.385	58.383	58.378	0.975	0.978	0.977	58.362	58.357	58.358	0.970	0.969	0.971
Image Zoom	-2	55.173	55.175	55.172	0.893	0.891	0.892	54.727	54.725	54.728	0.883	0.882	0.884

The results presented in Table 1 demonstrate the algorithm's robustness, measured by PSNR (dB) and NCC values, against multiple attacks. The PSNR values for Image 1 (R=67.563, G=67.562, B=67.565) and Image 2 (R=66.263, G=66.265, B=66.261) are exceptionally high, indicating no distortion under baseline conditions. The NCC values for both images across all channels are 1.000, signifying perfect correlation with the original images.

JPEG compression resulted in a reduction of PSNR to approximately 61.76 for Image 1 and 61.07 for Image 2, indicating moderate degradation in image quality. The NCC values (Image 1: R=0.945, G=0.946, B=0.944; Image 2: R=0.937, G=0.938, B=0.938) confirms a a high degree of similarity, though visible compression artifacts are introduced. Custom blur introduced a significant reduction in PSNR, with values of approximately 58.07 for Image 1 and 58.64 for Image 2. The NCC values remained high (Image 1: ≈0.955; Image 2: ≈0.985), reflecting the system's robustness to this type of distortion. Gaussian blur further degraded the PSNR to 57.64 (Image 1) and 56.92 (Image 2). However, the NCC values (Image 1: ≈0.966; Image 2: ≈0.935) indicate that structural integrity is largely preserved despite the visible blurring effects. Horizontal cropping caused the most substantial degradation, with PSNR values dropping to ≈51.07 (Image 1) and ≈51.08 (Image 2). The NCC values (Image 1: ≈0.889; Image 2: ≈0.871) were the lowest among all attacks, highlighting the sensitivity of the system to this type of spatial modification.

Vertical cropping had a relatively lesser impact on image quality, with PSNR values of ≈62.38 (Image 1) and ≈62.12 (Image 2). The NCC values (Image 1: ≈0.950; Image 2: ≈0.948) demonstrate the system's resilience to this attack, compared to horizontal cropping. Watermarking resulted in moderate reductions in PSNR, with values of ≈61.20 (Image 1) and ≈60.87 (Image 2). The NCC values (Image 1: ≈0.935; Image 2: ≈0.931) indicate visible but minor distortions in image similarity. Median filtering reduced the PSNR to ≈58.16 (Image 1) and ≈57.05 (Image 2), with NCC values remaining high (Image 1: ≈0.952; Image 2: ≈0.948). This suggests that while filtering introduces noise reduction artifacts, the overall similarity is maintained. Salt and pepper noise degraded PSNR to ≈58.38 (Image 1) and ≈58.36 (Image 2), with NCC values (Image 1: ≈0.977; Image 2: ≈0.970) demonstrating robustness against this type of attack. The results highlight the system's effectiveness in handling random noise. Image zoom caused a significant drop in both PSNR (Image 1: ≈55.17, Image 2: ≈54.73) and NCC (Image 1: ≈0.892, Image 2: ≈0.883). This attack introduced notable distortion, likely due to interpolation artifacts, demonstrating the sensitivity of the system to geometric transformations.

The experimental results show that the system achieves high PSNR and NCC values under baseline conditions, with minimal distortion and perfect similarity. Under attack scenarios, the performance varies. Compression, Noise, and Filtering introduce moderate degradation, with PSNR reductions of 5-10 dB and NCC values consistently above 0.93, highlighting the system's robustness to these attacks. Cropping and Zooming result in the most significant degradation, with PSNR values dropping by up to 16 dB and NCC values falling below 0.90. Horizontal cropping was particularly impactful, reflecting a potential weakness in handling spatial alterations. These results suggest that while the system demonstrates resilience to a wide range of attacks, spatial transformations such as cropping and zooming remain challenges that warrant further investigation.

5. CONCLUSION

In this research, a hybrid RGB blind watermarking scheme combining DWT, DCT, Arnold Transform, and ECDH Key Exchange was proposed to achieve secure and efficient watermarking. The algorithm demonstrated high imperceptibility and robustness against various attacks, providing reliable image authentication and copyright protection. The ICPAS system, built on this algorithm, enhances security and key management and therefore lays a strong foundation for secure digital watermarking solutions across industries like media, healthcare, and digital arts, addressing the growing need for reliable content protection in the evolving digital landscape. The proposed hybrid RGB blind watermarking scheme can be further enhanced to address emerging challenges in digital watermarking. Future research can focus on improving the algorithm’s robustness against geometric attacks like cropping and zooming, which remain challenging. The scalability of the system for real-time applications and large-scale datasets can also be explored to meet the demands of high-speed digital environments.

6. REFERENCES

[1] Phototutorial, "Statistics, Facts, & Predictions.," 2024. [Online]. Available: https://phototutorial.com/photos-statistics/. [Accessed 17 October 2024].

[2] Z. Heng , W. Chengyou and Z. Xiao , "Fragile Watermarking for Image Authentication Using the Characteristic of SVD," *Algorithms*, vol. 10, no. 1, p. 27, 2017.

[3] C. Ingemar, M. Miller, J. Bloom, J. Fridrich and T. Kalker, Digital watermarking and steganography, Morgan kaufmann, 2007.

[4] W. A. Fawaz , "Watermarking for Content Integrity and Ownership Control of Medical Images," *Journal of Artificial Intelligence*, vol. 10, pp. 32-41, 2017.

[5] R. Priyanka and S. Maheshkar , "Robust Multiple Composite Watermarking Using LSB Technique," in *inProceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory andApplications, Advances in Intelligent Systems and Computing*, 2017.

[6] M. Moosazadeh and G. Ekbatanifard, "Robust image watermarking algorithm using DCT coefficients rela-tion in YCoCg-R color space," in *Eighth International Conference on Information and KnowledgeTechnology (IKT)* , Hamedan, Iran, 2016.

[7] Y. Zhang , C. Wang and X. Zhou, "RST Resilient Watermarking Scheme Based on DWT-SVD and Scale-Invariant Feature Transform," *Algorithms*, vol. 10, no. 2, p. 41, 2017.

[8] R. Kefa, "Elliptic Curve Cryptography over Binary Finite Field GF(2m)," *Information Technology*, Vols. vol. 5,, pp. no.1, p. 204-229, 2006.

[9] P. Michal , P. K. Grzegorz and K.-J. Aleksandra, "YUV vs RGB – Choosing a Color Space for Human-Machine Interaction," in *2014 Federated Conference on Computer Science and Information Systems*, 2014.

[10] B. L. Gunjal and R. R. Manthalkar, "Discrete Wavelet Transform Based Strongly Robust Watermarking Scheme for Information Hiding in Digital Images," in *Third International Conference-Emerging Trends in Engineering and Technology*, Goa, India, 2010.

[11] G. L. Baisa and M. Suresh, "Secured color image watermarking technique in DWT-DCT domain," *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*, vol. 1, no. 3, 2011.

[12] R. Kefa, "Elliptic Curve Cryptography over Binary Finite Field GF(2m)," *Information Technology Journal*, Vols. 5, no.1, pp. 204-229, 2006.

[13] B. King, "An improved implementation of elliptic curves over gf(2n) when using projective point arithmetic," *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Arti_cial Intelligence and Lecture Notes in Bioinformatics), 2259(1)*, pp. 134-150, 2000.

[14] S. Mitchell D. and T. Ahmed H., Readings in Multimedia Computing and Networkng, 2002.

[15] S. H. a. E. C. Vidyasagar M. Potdar, "A Survey of Digital Image Watermarking Techniques," *in Proc. of the IEEE International Conference on Industrial Informatics*, pp. 709-716, 2005.