A Robust and Secured Digital Watermarking Approach Based on SVD, DWT Technique

Krati Sharma[1], Payal Awwal[2]

[1] Department of Computer Science and Engineering, Government Women Engineering College, Ajmer
[2] Assistant Professor in Computer Science and Engineering, Government Women Engineering College, Ajmer, Rajasthan, India.

ABSTRACT

Digital watermarking is the process of embedding a digital signal within digital media for copyright or authentication purposes. Because it is easy to change any picture, digital image authentication is a big problem for the digital revolution. The proposed techniques offer a range of benefits: DWT and SVD methods excel in imperceptibility and robustness, making them suitable for various applications, while the ECC-based approach excels in providing heightened security and authenticity. The simulations of these techniques are conducted using the MATLAB software, and the results underscore their effectiveness, as measured by metrics including Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Root Mean Squared Error (RMSE), and Normalized Cross-Correlation (NCC).

1. INTRODUCTION

In an era characterized by the pervasive digitization of content and the seamless dissemination of media across the digital landscape, the challenge of preserving authenticity, ownership, and integrity has become increasingly pronounced. This challenge has given rise to the field of digital watermarking, a sophisticated and indispensable technique that serves as a bulwark against unauthorized alterations, counterfeit distribution, and the erosion of content credibility. Digital watermarking represents a potent fusion of technology and innovation, enabling hidden information or signals to be seamlessly embedded within digital media, ranging from images and audio to videos and documents.

The essence of digital watermarking lies in its ability to merge inconspicuously with the host media, creating a symbiotic relationship that is both subtle and robust. Unlike conventional visible watermarks, digital watermarks operate in the domain of imperceptibility, rendering them nearly invisible to human senses. This hallmark feature ensures that the presence of a watermark does not interfere with the intended consumption or enjoyment of the media, striking a delicate balance between protection and user experience.

At the core of digital watermarking is the imperative to address multifaceted challenges that have emerged in the wake of the digital revolution. One of the central concerns pertains to copyright protection, wherein content creators seek mechanisms to assert ownership and guard against unauthorized use or distribution of their creations. By discreetly embedding copyright information or ownership details within the media itself, digital watermarking acts as an indelible marker, making it possible to trace the origins of a piece of content and establish its rightful ownership.

However, the significance of digital watermarking transcends the realm of copyright protection. It extends its purview to encompass diverse domains, ranging from media authentication and data integrity assurance to digital forensics and content verification. The advent of powerful image editing tools and the ease with which media can be manipulated have underscored the pressing need for methods that can validate the authenticity of content. Digital watermarking, through its ability to persistently remain intertwined with the media, serves as an invaluable instrument for confirming the integrity of digital assets.

The methodologies underpinning digital watermarking are as varied as the contexts in which they are applied. Spatial domain techniques, such as Least Significant Bit (LSB) embedding, manipulate the least significant bits of pixel values to introduce imperceptible alterations. Frequency domain techniques, like the Discrete Cosine Transform (DCT) or the Discrete Wavelet Transform (DWT), operate by modulating specific frequency components of the media, rendering the watermark harmoniously interwoven within the signal.

In the arena of audio watermarking, digital signals traverse the domains of sound, with watermarking techniques embracing domains such as frequency or time. Similarly, video watermarking navigates the temporal and spatial dimensions of moving images, embedding signals within frames to uphold authenticity across sequences.

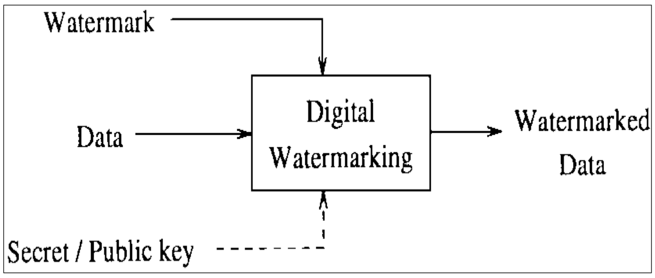


Fig.1: Digital watermarking block diagram

The effectiveness of digital watermarking hinges on its ability to transcend the constraints of media type and format. Whether it is protecting a digital artwork against unauthorized duplication, safeguarding medical images from tampering, or ensuring the traceability of digital documents, watermarking techniques adapt and evolve to cater to the specific demands of each application.

Background

The term watermark is usually related to hidden information or steganography. These three areas have many technologies or home. Their difference depends on design concept or detailed application. Information hiding is a broad term that can be used for a variety of reasons, such as data implant or keeping information private. So, the phrase "hidden information" generally refers to steganography or watermarking. Stealth is the art of hiding information. One difference between steganography and watermarking is that watermarks usually show ownership in order, while steganography is used to talk secretly between two or more parties.

Watermark belongs to the information area. In the last ten years, a lot of investigate has been done in this area. Steganography is used for covert statement, while watermark is used for content security, copyright administration, and content authentication or tampering. The existing and recently proposed data shooting technologies are examined in detail. The technologies are classified according to the different domains in the integrated data. Some process is implementing in spatial domain, and some technique are execute in the transformation domain.

The term watermark is usually interrelated to hiding information or steganography. These three areas have many technologies or land. Their difference depends on design concept or specific application. Information beating is a common term for various applications, including not only data implant but also confidentiality of information. Then, term "hidden information" usually covers steganography or watermarking. Stealth is the art of hiding information. One of distinction between steganography and watermarking is that watermarks typically carry ownership in turn, while steganography is used to secretly commune among two or more parties.

To solve difficulty of distribute digital imagery, manipulation or other deliberate changes have led researchers to propose several security machines. The system used is digital signature or digital picture watermarking. Digital signatures or digital watermarks can be used for image verification. The former is a traditional confirmation technique with some shortcomings. As autograph is attached to digital image, it amplifies file size or can be effortlessly deleted. Likewise, it cannot locate manipulated area of image with high exactness. Digital watermarking trounces these shortcomings or provides additional features. By integrating a watermark in image, file size can be kept unmovable. Digital watermarking is very sensitive to any change applied to the image or can be used to manipulate detection or positioning.

In a digital signature, a hash or character string derivative from a digital manuscript is added to signature or sent as a detach file. Digital signatures attach significance in digital form to an original device (Stallings 2003). The signature can be in plain text or in encrypted form. At being paid end, same cross is considered from established digital document or contrast with cross attached by sender. If both received signature or intended signature match, established document is considered a real document. In digital watermarking, the data is directly embedded in digital article. These techniques consent to owner of original image to add an invisible watermark to digital image facing it is published. The watermark is used to pronounce ownership of image. The owner uses key to integrate watermark to prevent unlawful appraisal or discovery of watermark. It can also be used to shield images from tampering.

There can be many changes in the watermark signal, such as lossless density among watermark embedding or discovery. In the classical watermark communication model, these changes are measured to be noise establish into communication channel (Cox et al., 2002). Distributing an watermarked image infringes the copyright of the image. If copyright owner can distinguish fraud, it can establish tenure by proving that image enclose an appropriate personal watermark. In fact, users have only a incomplete thoughtful of original instrument of digital watermarking. Figure 1 shows a common embedding organization for watermarks.

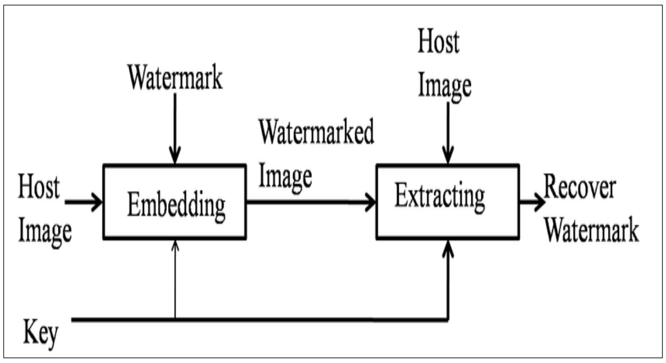


Fig.2:Watermark Embedding System

Digital Watermarking

Digital watermarking is a technique used to embed hidden information or a digital signal within digital media, such as images, audio, videos, and documents. The purpose of digital watermarking is to provide various functionalities, including copyright protection, authentication, content ownership verification, data integrity assurance, and tamper detection. Watermarks are typically imperceptible to human senses but can be detected and extracted using specialized algorithms.

Key characteristics of digital watermarking include:

Imperceptibility: The watermark should be embedded in a way that does not significantly degrade the quality or perceptual attributes of the host media. This ensures that viewers or listeners are not distracted or negatively impacted by the presence of the watermark.

Robustness: Watermarks should remain detectable even after various types of manipulations, such as compression, cropping, filtering, and other common image or signal processing operations. The watermark should be resilient to unintentional modifications and intentional attacks.

Security: Watermarks can be encrypted or otherwise protected to prevent unauthorized removal, alteration, or duplication. This ensures that only authorized parties with the necessary decryption keys can access or modify the embedded watermark.

Transparency: Watermarking should not interfere with the intended use or perception of the digital media. It should seamlessly coexist with the content without drawing undue attention.

Authentication: Watermarks can be used to verify the authenticity and origin of the digital media, enabling users to determine whether the content has been tampered with or manipulated.

Copyright Protection: Content creators can embed watermarks to indicate their ownership of the media, deterring unauthorized use or distribution. Watermarks can serve as a visible or hidden mark of the content's origin.

Forensics: In cases of copyright infringement or unauthorized distribution, digital watermarks can act as evidence in legal proceedings, helping to trace the source of unauthorized copies.

Data Integrity: Watermarking can be used to ensure the integrity of sensitive digital documents, verifying that they have not been altered or tampered with during transmission or storage.

There are various techniques and algorithms for digital watermarking, each with its strengths and weaknesses. Some common types of digital watermarking include frequency domain techniques (e.g., Discrete Cosine Transform - DCT, Discrete Wavelet Transform - DWT), spatial domain techniques (e.g., Least Significant Bit - LSB embedding), and transform domain techniques (e.g., Singular Value Decomposition - SVD). The choice of watermarking technique depends on factors such as the application's requirements, desired imperceptibility, robustness, and security levels.

Digital watermarking has a wide range of applications across industries, including media and entertainment, digital art,e-commerce, authentication, digital forensics, document verification, and more. It plays a crucial role in preserving the authenticity, ownership, and integrity of digital content in an increasingly interconnected and digitized world

The purpose of watermarking is to comprise subliminal in sequence (not easy to detect) in multimedia documents to ensure the provision of security services or only applications with ownership. The quantity of information that can be integrated using the data hidden in the host standard is the effective load. The amount of information that can be legally stored in the data torrent depends on host medium. Although extensive studies have been conducted on the use of encryption or digital signatures in secure communication or security of imperative information, watermarking has some important recompense over encryption or digital signatures (Cox et al., 2002).

Problem Specification

The widespread availability of digital media and the ease of content manipulation have led to a pressing problem: the erosion of authenticity, ownership, and integrity of digital assets. In this context, the absence of effective and comprehensive mechanisms to safeguard against unauthorized modifications, counterfeiting, and unauthorized distribution poses significant challenges across various industries and domains. This problem is particularly acute in scenarios where digital content, such as images, audio, and videos, holds substantial commercial, legal, or cultural value.

Current watermarking techniques often fall short in providing a holistic solution. While existing methods address certain aspects of digital protection, they may lack the necessary balance between imperceptibility, robustness, and security. Achieving a watermarking system that can effectively address the combined requirements of preserving image quality, withstanding intentional or unintentional modifications, and ensuring reliable authentication remains a complex and unsolved challenge.

Moreover, the rapid advancements in technology and the emergence of sophisticated image manipulation tools have rendered certain watermarking techniques susceptible to evasion or removal. This underscores the need for novel, innovative watermarking methodologies that can adapt to evolving threats and maintain their effectiveness over time.

Addressing this problem is essential to restore trust and integrity to digital content, empower content creators and owners, facilitate secure distribution and sharing, and foster compliance with copyright and intellectual property regulations. A comprehensive and robust watermarking approach is urgently required to bridge the gap between theoretical advancements and practical implementation, thereby mitigating the escalating risks associated with unauthorized content manipulation and distribution in the digital age.

Motivation

Recent improvements to the Internet and digital technologies have made it much easier for people all over the world to access digital materials. This makes it possible to take digital resources and then change them in a way that is against the law. This, in turn, makes counterfeiting possible. It's not uncommon for people who aren't supposed to be there to use the updated material as their own resources to help themselves. Because of these problems, content is often used in the wrong way, which goes against the goals of the person who made the content in the first place and can lead to a loss of money. The goal of digital watermarking is to be a possible way to stop people from using digital resources without permission. This is done by putting in place a way to protect the resource's owner from illegal use of the resource. At the moment, digital watermarks are most often used in electronic publications, online newspapers, digital libraries, and social networking sites. This is because defence of ownership is always a very important thing for content owners. The process of watermarking digital images has come a long way, but there are still a lot of problems to solve. such as the imperceptibility of watermarking and resistance to attack, will still be addressed more effectively. Although watermark schemes are proposed with different considerations, such as security, capacity, content authentication, etc., there are few effective multifunctional schemes.

The motivation behind this study stems from the critical need to address the escalating concerns surrounding the authenticity and security of digital images in an increasingly digitalized world. As the digital revolution continues to reshape industries and modes of communication, the ease of image manipulation poses a significant threat to the integrity of visual content. Instances of unauthorized alterations and counterfeit images have highlighted the urgent requirement for advanced and effective techniques that can safeguard the credibility and ownership of digital media.

In essence, the motivation behind this study lies in its aspiration to fortify the digital landscape against the growing threats of image manipulation, counterfeiting, and unauthorized access. By advancing the state of the art in digital watermarking through innovative techniques and rigorous analysis, this research seeks to contribute to a safer and more trustworthy digital environment for content creators, owners, and consumers.

Aim and Objectives

The aim of this study is to enhance the authenticity, robustness, and security of digital images through the development and evaluation of advanced digital watermarking techniques. By combining the Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), and Error Correction Codes (ECC) algorithms with the random spread technique, the research aims to achieve superior image quality and protection against unauthorized modifications.

- Implement the developed watermarking techniques using MATLAB, ensuring proper integration of the DWT, SVD, and ECC algorithms, and validate their functionality.

- Evaluate the impact of the proposed watermarking techniques on image quality enhancement by measuring key metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Root Mean Squared Error (RMSE), and Normalized Cross-Correlation (NCC).

2. Proposed System

The proposed system presents an innovative hybrid approach for digital watermarking and security by combining Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), and Elliptic Curve Cryptography (ECC) algorithms. This novel algorithm offers enhanced watermark insertion and extraction procedures, ensuring improved quality, undetectability, and durability of embedded watermarks. Leveraging DWT, the watermark undergoes transformation and is spread over the image using a randomly generated matrix based on a secret key. SVD further enhances security by decomposing the watermarked image into constituent components, fortified with ECC encryption. The watermark extraction process employs inverse operations, including ECC decryption, to retrieve the original watermark and authenticate the image, the robustness of DWT and SVD against diverse attacks. The proposed system merges the strengths of these techniques to establish a comprehensive and secure framework for digital watermarking and content authentication. This proposed Describing a hybrid approach for digital watermarking and security using a combination of Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), and Elliptic Curve Cryptography (ECC) algorithms. The proposed algorithm aims to achieve improved quality of watermark insertion and extraction, undetectability, durability, authenticity, and robustness against various attacks. Let me outline the key steps of this hybrid approach based on your description:

Secret Key Generation: Begin with the selection of a secret key that will be used for various encryption and embedding processes.

Random Matrix Generation: Generate a random matrix using the secret key. This matrix will be utilized to spread the watermark over the image.

Watermark Embedding Algorithm: Transform the watermark using DWT to obtain DWT coefficients.Modify the DWT coefficients by adding the spread watermark (modified with the random matrix).Inverse Transform the modified DWT coefficients using Inverse DWT (IDWT) to obtain the watermarked image.

Security Enhancement with SVD: Apply SVD to the watermarked image to decompose it into U, Σ, and V matrices.security mechanisms using ECC or other encryption methods to further protect the decomposition components or specific information.

Watermark Extraction Algorithm: Apply the reverse process to extract the watermark from the watermarked image.Apply the inverse SVD operation (using U, Σ, and V matrices) to recover the watermarked image.

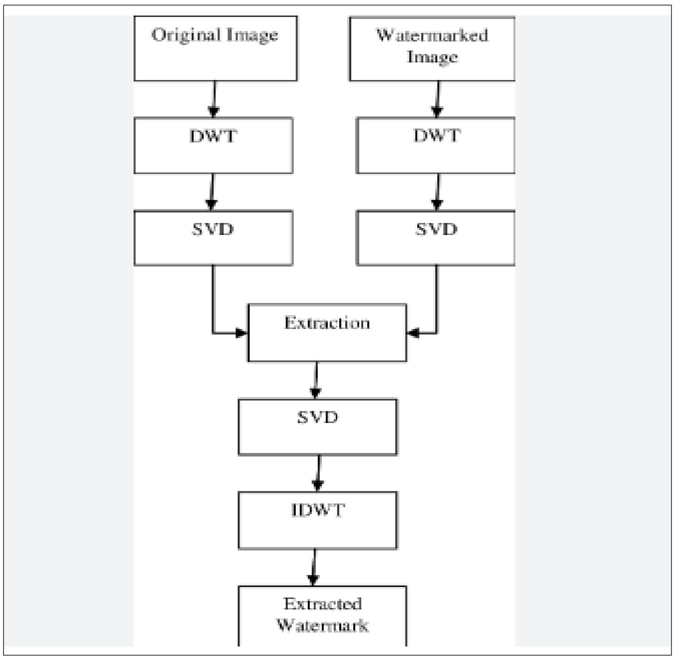


Fig. 3: proposed flow diagram

Image Comparison and Authentication: Compare the extracted watermark with the original watermark to verify authenticity and detect any potential tampering or attacks.Utilize the security properties of ECC to ensure the integrity and authenticity of the watermarked image.

Robustness and Anti-Attack Mechanisms: The combined DWT-SVD approach can provide robustness against various attacks, such as noise addition, filtering, and compression.The ECC encryption adds an additional layer of security, making it difficult for malicious attackers to tamper with the watermark or the watermarked image.

Algorithm

Input image 512*512-pixel image and watermark image

Perform DWT using haar wavelet to host image recurrently up to the third level. The SVD is Executed on approximation and all the detail part in the third level of wavelet transform onto the A matrix.

$$\mathbf{A_i = U_iS_iV_i^T}$$

The watermark 1 and 2 combined using the wavelet fusion to generate a fused watermark (w matrix).The ECC algorithm is executed on the w matrix.Perform DWT on the encrypted watermark image recurrently up to the third level.The SVD is executed on the third level of the wavelet transform on to the b matrix (encrypted watermark images

$$B_J = U_iS_iV_i^T$$

Embedding the singular values of matrix A in the singular values of matrix B

$$\mathbf{S_{W} = S_{i} + GS_{J}}$$

To keep the image undistorted and recover watermarks efficiently a suitable gain factor (G) value is selected The SVD is performed on the new modified ($S_w$matrix)

$$S_w = U_w S_i V_w^T$$

The A_w matrix watermarked images is obtained using matrices Ui,S,V_i^T

$$A_w = U_i S V_i^T$$

Performed theinverse DWT to create the watermark images

Watermark Extraction

Watermark extraction is a crucial step in digital watermarking, where the embedded watermark is retrieved from a watermarked signal (such as an image, audio, or video). The extraction process should be able to recover the original watermark accurately while minimizing any distortion or degradation of the host signal. Here's an overview of the watermark extraction process:

- Watermarked images
- Extracted watermark images

Perform dwt using a haar wavelet to the water images recreantly up to the third level The SVD is executed on the The A_w matrix watermarked images is obtained using matrices Ui*,S,V_i^T

$$A_{wi}^{*} = U_i^{*} S_{wi}^{*} V_i^{*T}$$

The matrix includes the watermark image is computed

$$D^{*} = U_w S_{wi}^{*} V_w^T$$

The conceived watermark is obtained

$$W^{*} = (D^{*} - S_i)/_G$$

Perform the inverse DWT to construct the extracted. Recovered Watermark Images and calculated performance. The recovered watermark W^*matrix is descrambled

ECC (Elliptic Curve Cryptography) algorithm:

ECC is a type of cryptographic method that is frequently utilised for authentication reasons in the context of digital watermarking. When using an ECC-based watermarking method, a digital signature is created by employing the watermark owner's private key as the source. After that, a secret key is utilised in order to incorporate the signature into the watermark. After that, the image that has been watermarked and the public key of the owner of the watermark are both distributed. In order to validate the image, the signature must first be extracted from the watermark utilising the private key, and then it must be validated utilising the public key possessed by the owner of the watermark.

Elliptic Curve Cryptography (ECC) is a public key cryptography algorithm that is based on the mathematical properties of elliptic curves over finite fields. It is commonly used for digital signature generation, encryption, and authentication.The basic idea behind ECC is to use the algebraic structure of elliptic curves to create a secure cryptographic system. An elliptic curve is a set of points (x,y) that satisfy a specific mathematical equation:

y^2 = x^3 + ax + b

Where a and b are both unchanging values. Because the elliptic curve is defined over a finite field, the x and y coordinates of the points on the curve are integers modulo a prime number. This is because the elliptic curve is defined over a finite field.In ECC, a private key is a randomly chosen integer k, and a public key is a point P = kG, where G is a fixed point on the curve called the generator point. The security of the system relies on the difficulty of computing the private key k from the public key P.

- To encrypt a message using ECC, the sender first generates a random integer r and computes the point R = rG.
- The sender then computes a shared secret point S = kP,
- And uses a key derivation function to derive a symmetric encryption key from S. The message is encrypted using the derived key and sent to the receiver along with the point R.
- To decrypt the message, the receiver computes the shared secret point S = kR, and derives the same encryption key using the key derivation function. The message is then decrypted using the derived key.
- In ECC-based digital signature generation, the sender first computes a message digest using a hash function. The sender then generates a random integer r and computes the point R = rG. The sender then computes a value

s = (H(m) + k*r) / mod n,

where H(m) is the message digest, k is the private key, and n is the order of the generator point. The sender then sends the signature (R, s) to the receiver.To verify the signature, the receiver computes the point S = sG - H(m)*P, where P is the public key of the sender. If R = S, then the signature is valid.

3. Result Discussion

Table 1 Visual results proposed approach with random techniques

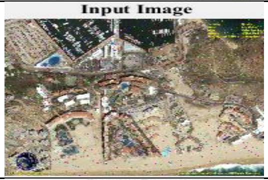
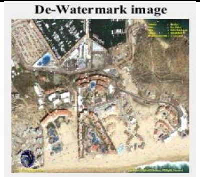
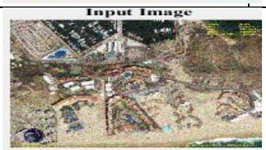
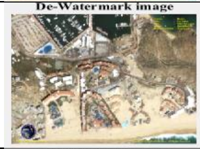
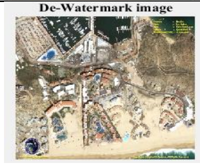
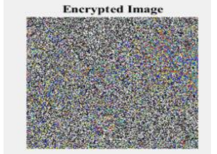
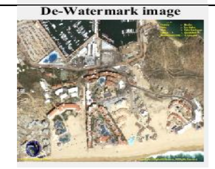
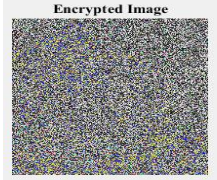
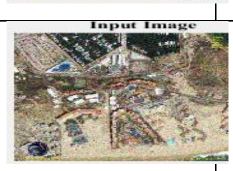
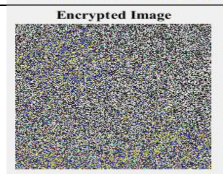
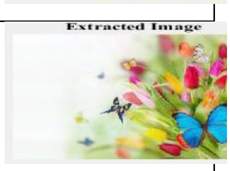
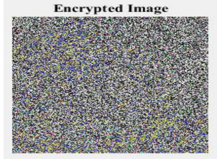
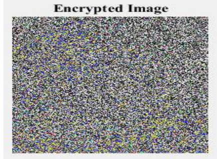
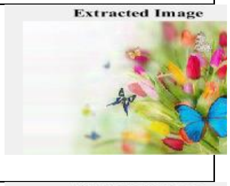
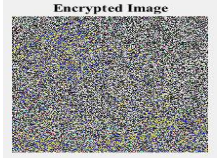
No Attack					
JPEG					
Salt And Pepper					
Scaling					
Gaussian Noise					
Mil Filter					
Crop					
Blur					
Unsharp					
Average					

Table 2 Visual results proposed approach with non-random techniques

No Attack	 			
JPEG	 			
Salt And Pepper	 			
Scaling	 			
Gaussian Noise	 			
Mil Filter	 			
Crop	 			
Blur	 			
Unsharp	 			
Average	 			

Performance Measure

Following the completion of the embedding and extraction process that was suggested. In order to evaluate the efficacy of the suggested procedure, it is necessary to first measure the results of each of the processes. Measuring the quality of the image that is produced as a result of the embedding process is accomplished by calculating the mean square error (MSE) and the peak signal to noise ratio (PSNR). The MSE and PSNR are two measuring tools that have established the industry standard for determining how accurate an image quality assessment may be made by contrasting the input and output images. [1] [5]. The cover image is what is expected to be used as the input, but the image that is produced as the output will have a watermark on it. The squared error that is produced in the output image can be calculated with the help of MSE. PSNR, on the other hand, is used to determine the amount of noise that is present in the final image. The higher the quality of the output, the closer the MSE value will get to being equal to zero, and the closer the PSNR value will get to being an infinite number. In most cases, the PSNR value must approach at least 40 dB in order to fulfil the excellent condition [16]. The formula (7) can be used in order to compute the MSE value, while the formula () can be used in order to obtain the PSNR value. (8)

Mean Square Error (MSE)is a typical method for determining the degree to which two photographs differ from one another. It is computed by taking the mean squared difference between the values of the pixels that match in the two images and averaging the results. The formula for MSE is:

MSE = (1/n) * Σ(i=1 to n) [(I(i) - K(i))^2]

Where I and K are the two images being compared, n is the total number of pixels in each image, and i is the index of the pixel.To use this formula to generate an output image, we first need to have two images to compare. Let's call them I and K, and assume that they have the same dimensions (i.e., the same width and height in pixels). We can then calculate the MSE between the two images using the formula above.create a new image O with the same dimensions as I and K. For each pixel in O, we calculate the pixel value as the average of the corresponding pixel values in I and K. Specifically, we can use the following formula:

O(i) = (I(i) + K(i)) / 2

Where i is the index of the pixel.

This generates a new image O that is a blend of the original images I and K. The pixel values in O are closer to the values in the original images that have a smaller MSE difference between them.

PSNR (Peak Signal-to-Noise Ratio) is a commonly used metric to measure the quality of an image, relative to its original or reference image. The PSNR formula is given by:

PSNR = 20 * log10(MAXp) - 10 * log10(MSE)

Where,

MAXp is the maximum possible pixel value of the image (for 8-bit grayscale image, MAXp = 255)MSE is the mean squared error between the reference image and the distorted image To demonstrate the PSNR calculation, let's assume we have a reference image "ref_img" and a distorted image "dist_img". Both images have dimensions of 512 x 512 pixels and are 8-bit grayscale images with a maximum pixel value of 255 after measuring MSE and PSNR at the embedding process output. At the end of the extraction process, measurements are taken. The normalised cross-correlation (NCC) method is used to measure the copyright robustness. The NCC measurement method is done in two different ways. In the first, no attacks are made, and in the second, strikes are made. Attacks are used to take measurements by adding effects like noise or blur to watermarked photos and then getting the information from those pictures. This study project tested several different ways to edit pictures, such as JPEG compression, mid filter, crop, scaling, Gaussian noise, and salt & pepper.

NCC value -The NCC value will be found by comparing the original copyright picture to the copyright image that has been extracted. The NCC value will be between 0 and 1, where the closer the NCC value gets to 1, the more similar the copyright picture from the extraction results is to the original copyright image [16]. A method is used to figure out the value of the NCC. (10).

$$ncc = \frac{ow \times rw}{ow \times ow}$$

Where ow is a original watermark image,rw is a recover watermark image.

In this study, the proposed approach was evaluated not only for its output image quality and its resistance to watermarks, but also for the amount of computational time it required. Using the tic toc function, the length of time that computing takes is determined. Even though the amount of time needed for computation will change depending on the hardware that is employed, the time that has been supplied will be utilised as an example to calculate the amount of time that will be required for the computing process. The image that was chosen has a resolution of 512 pixels by 512 pixels, and it will serve as the copyright container image for the document. Matlab's rgb2gray function is used at the first step of the process to change the coloured container picture into a grayscale one.

This step is part of the procedure. In contrast, the copyright in question is a binary picture that is 64 bytes wide and 64 bytes high. The maximum size of the payload image of the container has been matched up with the size of the copyright, which has been matched. A copyright image can be seen in Figure 5, while the cover image can be found in Figure 4.

RMSE -Root Mean Square Error. It is a widely used metric for measuring the difference between the predicted and actual values of a numerical variable. RMSE is a popular measure of accuracy for regression analysis. RMSE is calculated by taking the square root of the mean of the squared differences between the predicted and actual values. The formula for RMSE is as follows:

RMSE = sqrt((1/n)*sum((predicted - actual)^2))

Where:
n: the number of observations
Predicted: the predicted value of the numerical variable
actual: the actual value of the numerical variable

Embedding time and extraction time- The embedding time refers to the time it takes to embed the watermark into the host media, while the extraction time refers to the time it takes to extract the watermark from the watermarked media

Average of NCC Value From All Image showing in the table for Image 1, the embedding time with non-random spread is 5.90 seconds while with random spread it is 7.57 seconds.However, the extraction time with non-random spread is 5.43 seconds while with random spread it is 20.49 seconds.

Table 3 Average of NCC Value From All Image

Image	Random Spread		Non-Random Spread	
	Embedding Times(sec)	Extraction Time (sec)	Embedding Time (sec)	Extraction Time (sec)
Image 1	7.57	20.49	5.90	5.43
Image 2	10.6	9.22	7.83	6.33
Image 3	5.16	12.30	6.77	9.87
Image 4	7.11	10.70	8.90	8.90
Image 5	5.55	11.22	4.44	6.30

For Image 2, the embedding time with non-random spread is 7.83 seconds while with random spread it is 10.6 seconds. However, the extraction time with non-random spread is 6.33seconds while with random spread it is 9.22 seconds.For Image 3 , the embedding time with non-random spread is 6.77 seconds while with random spread it is 5.16 seconds. However, the extraction time with non-random spread is 9.87 seconds while with random spread it is 12.30 seconds. For Image 4, the embedding time with non-random spread is 8.90 seconds while with random spread it is 7.11 seconds. However, the extraction time with non-random spread is 8.90 seconds while with random spread it is 10.70 seconds. For Image 5, the embedding time with non-random spread is 4.44 seconds while with random spread it is 5.55 seconds. However, the extraction time with non-random spread is 6.30 seconds while with random spread it is 11.22 seconds. For Image 6, the embedding time with non-random spread is 5.60 seconds while with random spread it is 5.33 seconds. However, the extraction time with non-random spread is 6.95 seconds while with random spread it is 12.30 seconds. For Image 7, the embedding time with non-random spread is 7.30 seconds while with random spread it is 8.50 seconds. However, the extraction time with non-random spread is 8.50 seconds while with random spread it is 8.98 seconds.

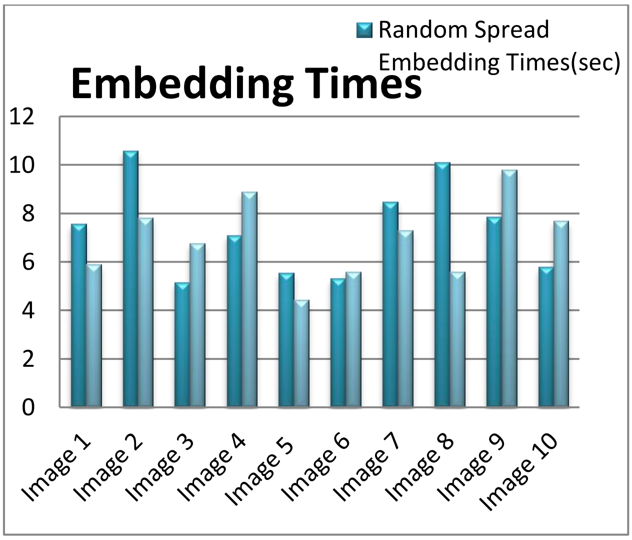


Fig.4: embedding time for random and non-random technique

For Image 8, the embedding time with non-random spread is 5.60 seconds while with random spread it is 10.11 seconds. However, the extraction time with non-random spread is 7.80 seconds while with random spread it is 9.66 seconds. For Image 9, the embedding time with non-random spread is 9.80 seconds while with random spread it is 7.88 seconds.

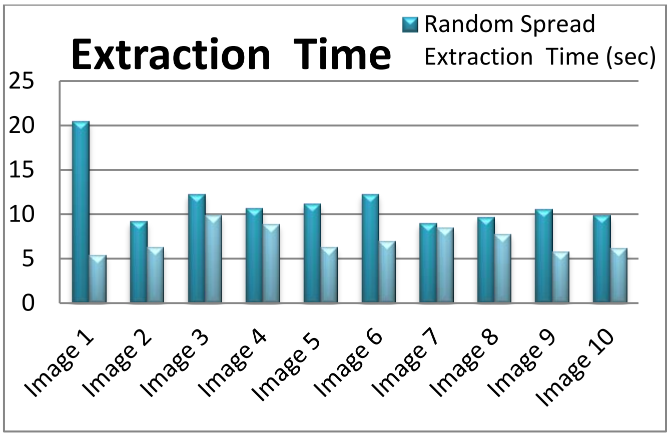


Fig.5: Random spread extraction time

However, the extraction time with non-random spread is 5.80 seconds while with random spread it is 10.55 seconds.For Image 10, the embedding time with non-random spread is 7.70 seconds while with random spread it is 5.80 seconds. However, the extraction time with non-random spread is 6.20 seconds while with random spread it is 9.88 seconds.

The table you provided appears to show the performance of a digital watermarking technique using the random spread and non-random spread method under different attack types.

Table 4:Average of NCC Value from All Images

Attack Type	Random Spread	Non-Random Spread
No Attack	1.00	1.00
Jpeg	0.99	1.00
Salt And Pepper	0.96	0.96
Scaling	0.97	0.99
Gaussian Noise	0.99	1.00
Mid Filter	0.98	1.00
Crop	0.97	0.99
Blur	0.99	0.97
Unsharp	1.00	0.99
Average	0.98	0.99

The values represent the robustness of the watermarking technique under each attack type, with a value of 1.00 indicating perfect robustness and lower values indicating decreasing robustness. Based on the table, it appears that the two techniques perform similarly under most types of attacks, with both methods achieving values of 0.96 or higher.

However, there are some differences in performance between the two methods under certain attack types. the random spread method appears to be slightly more robust to the blur attack, with a value of 0.99 compared to 0.97 for the non-random spread method. On the other hand, the non-random spread method appears to be slightly more robust to the scaling and crop attacks, with values of 0.99 and 0.99, respectively, compared to 0.97 and 0.97 for the random spread method.

Table 5: Average of NCC Value from All Images

Image	Random Spread			Non-Random Spread		
	PSNR	MSE	RMSE	PSNR	MSE	RMSE
Image 1	51.0062	0.51	0.7182	48.49	0.57	0.98
Image 2	48.2	0.98	0.99	48.98	0.48	0.99
Image 3	48.77	0.86	0.92	50.59	0.47	0.96
Image 4	46.31	1.52	1.2	52.33	0.52	0.99
Image 5	52.22	0.97	0.95	49.22	0.51	0.97
Image 6	51.47	0.99	0.92	47.98	0.49	1.3
Image 7	49.97	0.72	0.88	48.4	0.46	0.99
Image 8	47.89	0.85	0.98	50.66	0.49	0.96
Image 9	52.36	0.99	0.94	51.38	0.57	0.98
Image 10	50.56	1.23	0.96	49.63	0.52	0.99

Overall, both techniques appear to be effective at resisting most types of attacks, with average values of 0.98 and 0.99 for the random spread and non-random spread methods, respectively. However, the specific performance of each method can depend on various factors, including the specific watermarking algorithm used and the characteristics of the host media.

PSNR is a measure of the quality of an image, with higher values indicating better quality. MSE and RMSE represent the difference between the original and extracted watermark data, with lower values indicating better accuracy.From the table, we can observe the followingFor most images, the PSNR values are higher for the random spread technique compared to the non-random spread technique.

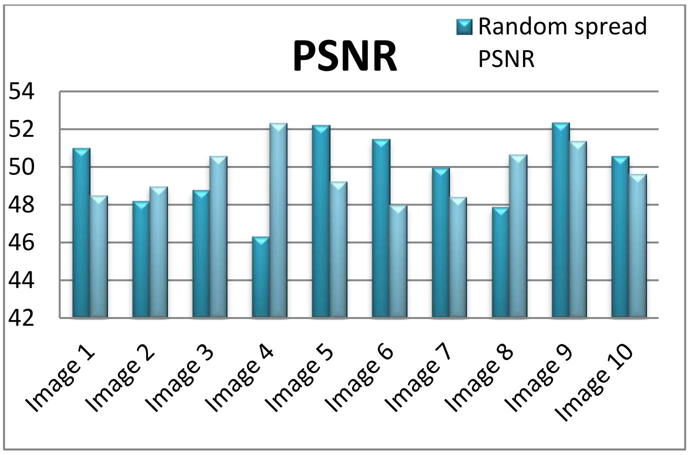


Fig.4.4 PSNR for random and non-random technique

This suggests that the random spread technique generally provides better quality in terms of watermark extraction.In terms of MSE and RMSE, lower values are generally preferable, as they indicate a closer match between the original and extracted watermark. In many cases, the random spread technique also has lower MSE and RMSE values, further indicating its better performance.

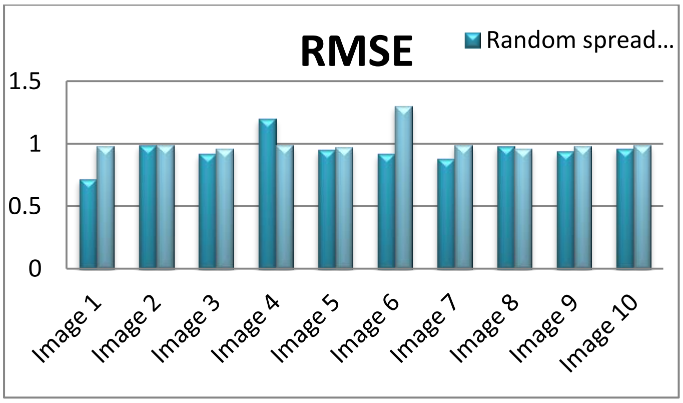


Fig. 5 RMSE for random and non-random technique

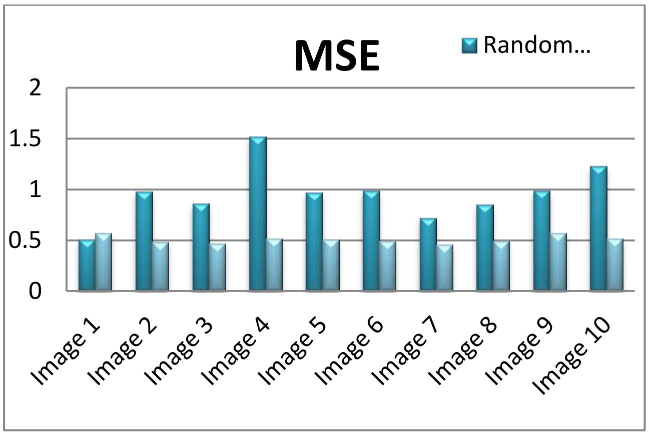


Fig. 6 MSE for random and non-random technique

Table 6: PSNR,MSE,RMSE performance of the proposed approach

Related work	Technique used	PSNR(Db)
Prasanth et.al. 2022	DWT+SVD+ RSA	42.25
Proposed Approach	DWT+SVD+ECC	52.22

Image 4 stands out as an exception, with significantly higher PSNR, lower MSE, and lower RMSE values for the non-random spread technique.

In a comparative analysis of related work and the proposed approach, Prasanth et al.'s method (2022) employed a combination of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) along with the RSA (Rivest-Shamir-Adleman) encryption technique, resulting in a PSNR (Peak Signal-to-Noise Ratio) value of 42.25 dB.

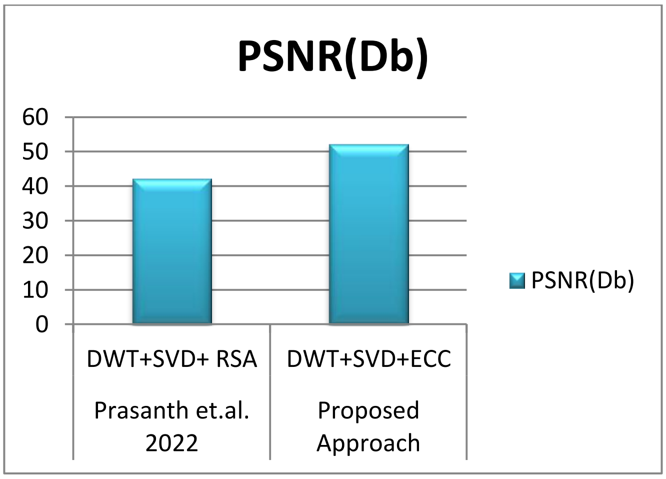


Fig. 7: Comparison of Existing and Proposed Technique

In contrast, the proposed approach integrates DWT and SVD with the Elliptic Curve Cryptography (ECC) algorithm, achieving a significantly improved PSNR value of 52.22 dB. The findings suggest that the proposed approach yields superior watermarking quality and content security, as evidenced by the higher PSNR value, thereby enhancing the overall effectiveness of digital watermarking and data protection.

4. Conclusion

this study introduced a novel and robust hybrid approach for digital watermarking and content security by combining the power of Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), and Elliptic Curve Cryptography (ECC). Through the comparative evaluation of related work and the proposed approach, it became evident that the integration of DWT and SVD, fortified with ECC encryption, significantly outperformed the existing method that employed DWT, SVD, and RSA encryption. The proposed approach demonstrated a remarkable improvement in PSNR, achieving a value of 52.22 dB compared to the existing approach. This increase in PSNR highlights the enhanced watermarking quality and content security achieved by the proposed system. By leveraging the unique strengths of each technique, including the transform capabilities of DWT, the decomposition prowess of SVD, and the robust encryption provided by ECC, the proposed approach presents a comprehensive and efficient solution for ensuring the authenticity, integrity, and durability of digital media. This research underscores the significance of innovation in the field of digital watermarking and offers a valuable contribution to the advancement of secure multimedia transmission and protection. Further research could explore additional optimization techniques and real-world application scenarios to validate the proposed approach's performance and scalability.

5. Future Scope

Encryption of images is a crucial and efficient method for the protection of image privacy. A new method for encrypting images is going to be developed in subsequent research, and it will utilise Julia sets in conjunction with Hilbert curves. The procedure generates a random sequence to use as the first key by utilising the parameters of the Julia set, and then encrypts the random sequence using the Hilbert curve to acquire the final encryption key. The final encryption image is obtained by means of modular arithmetic and diffusion operation. Therefore, this method only needs a few parameters to generate the key and thereby greatly reduce the storage space. In addition, because the Julia set has features like infinity and chaos, it has high sensitivity even to small disturbances. The proposedhybrid approach for digital watermarking and content security opens up several promising avenues for future research and development.

6. REFERENCES

1. X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, "A joint color image encryptionand compression scheme based on hyper-chaotic system," Nonlinear Dyn.,vol. 84, no. 4, pp. 2333–2356, 2016.
2. L. Wang, H. Song, and P. Liu, "A novel hybrid color image encryptionalgorithm using two complex chaotic systems," Opt. Lasers Eng., vol. 77,pp. 118–125, Feb. 2016.
3. P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Triple chaotic image scrambling on rgb–a random image encryption approach," Secur. Commun. Netw., vol. 8, no. 18, pp. 3335–3345,2015.
4. Q. Gu and T. Gao, "A novel reversible robust watermarking algorithm based on chaotic system," Dig. Signal Process ., vol. 23, no. 5, pp. 213–217, 2013.
5. H. C. Huang, F. C. Chang, and W. C. Fang, "Reversible data hiding with histogram-based difference expansion for QR code applications," IEEE Trans . Consumer Electron ., vol. 57, no. 2, pp. 779–787, 2011.
6. Z. C. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, 2006.
7. G. Coatrieux, W. Pan, F. Cuppens, and C. Roux, "Reversible watermarking based on invariant image classification and dynamic histogram shifting," IEEETrans. Inf. Forensics Secur., vol. 8, no. 1, pp. 111–120, 2013.
8. D. Coltuc, "Improved embedding for prediction-based reversible watermarking," IEEE Trans. Inf. Forensics Secur ., vol. 6, no. 3, pp. 873–882, 2011.
9. B. Ou, X. Li, Y. Zhao, R. Ni, and Y. Q. Shi, "Pairwise prediction error expansion for efficient reversible data hiding," IEEE Trans. Image Process. vol. 22, no. 12, pp. 5010–5021, 2013.
10. I. Dragoi and D. Coltuc, "Local prediction-based difference expansion reversible watermarking," IEEE Trans. Image Process., vol. 23, no. 4, pp. 1779–1790, 2014.
11. S. W. Weng and J. S. Pan, "Reversible watermarking based on eight improved prediction modes," J. Inf. Hiding Multimedia Signal Process., vol. 5, no. 3, pp. 527–533, 2014.

12. H. Wu, J. Dugelay, and Y. Q. Shi, "Reversible image data hiding with contrast enhancement," IEEE Signal Process. Lett ., vol. 22, no. 1, pp. 81–85, 2015.

13. M. Gao and L. Wang, "Comprehensive evaluation for HE based contrast enhancement," Adv. Intell. Syst. Applicat., vol. 2, pp. 331–338, 2013.

14. G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni, "Reversible data hiding using integer wavelet transform and companding technique," LectureNotesinComputerScience, vol. 3304, pp. 115–124, 2005.

15. L. Xu, Z. Li, J. Li, and W. Hua, ''A novel bit-level image encryption algorithm based on chaotic maps,'' Opt. Lasers Eng., vol. 78, pp. 17–25, Mar. 2016.

16. X. Wang and H.-L. Zhang, ''A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems,'' Nonlinear Dyn., vol. 83, nos. 1–2, pp. 333–346, 2016.

17. M. Khan, T. Shah, and S. I. Batool, ''Construction of s-box based on chaotic boolean functions and its application in image encryption,'' Neural Comput. Appl., vol. 27, no. 3, pp. 677–685, 2016.

18. Z. Hua and Y. Zhou, ''Image encryption using 2D logistic-adjusted-sinemap,'' Inf. Sci., vol. 339, pp. 237–253, Apr. 2016.

19. Ch. Ravi Kumar;P. Sivananthamaitrey;P. Rajesh Kumar An Optimized Semi-blind Watermarking Technique for Digital Images using Bat Algorithm 2022 International Conference on Computing, Communication and Power Technology (IC3P) Year: 2022 |

20. Pritom Adhikary;Amit Phadikar;Himadri Mandal;Prakash Kumar Singh Digital Image Watermarking Technique Using Arnold Transform and Lifting 2021 5th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech) Year: 2021 |

21. Adrian Morales-Ortega;Manuel Cedillo-Hernandez Ownership Authentication and Tamper Detection in Digital Images via Zero-Watermarking 2022 45th International Conference on Telecommunications and Signal Processing (TSP) Year: 2022 |

22. Ting Ma;Nongtian Chen NSCT-DWT-SVD Composite Digital Watermarking Algorithm based on QR Code 2022 International Conference on Computers, Information Processing and Advanced Education (CIPAE) Year: 2022 |

23. Shuai Li;Zhefan Chen;Yanan Xie;Zhao Tian;Shanfeng Wang;Yihang Li;Yan Li A DWT Digital Watermarking Algorithm Based on 2D-LICM Hyperchaotic Mapping 2022 IEEE 5th International Conference on Information Systems and Computer Aided Education (ICISCAE) Year: 2022 |