ISSN : 2455-9679
SJIF Impact Factor : 6.008

IJRTSM
INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"DESIGN AND DEVELOPED A DIGITAL WATERMARKING SECURITY SYSTEM BASED ON DWT-SVD AND ECC ALGORITHM"

Ramesh Kumar [1], Prof. Varsha Thakur [2]
[1] *M.Tech Scholar, Mittal Institute of Technology, Bhopal, India*
[2] *Assistant Professor, Mittal Institute of Technology, Bhopal, India*
rameshpadmakar7683@gmail.com, Anantha.thakur@gmail.com

ABSTRACT

Digital watermarking is a process used to embed a digital signal into digital media, primarily for purposes such as copyright protection and authentication. In the era of digital technology, ensuring the trustworthiness of digital images has become a significant challenge due to the ease of image manipulation. Researchers have been actively addressing this concern over the past three decades, developing various watermarking techniques tailored to specific applications. Nevertheless, creating a watermarking system that simultaneously achieves robustness and security remains a formidable task. In this dissertation, a novel digital watermarking approach is proposed, employing a combination of the Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), and Error Correction Codes (ECC) algorithms. This approach is complemented by the use of the random spread technique, known to enhance the quality of the resulting output images. The watermarking process involves distinctive methodologies for each algorithm: SVD-based watermarking involves modifying the singular values of the host image. DWT-based watermarking focuses on altering the coefficients of the high-frequency sub-bands of the host image. ECC-based watermarking generates a confidential digital signature using the owner's private key, which is then embedded within the watermark using a secret key. The proposed techniques offer a range of advantages: 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 MATLAB software, and the results demonstrate 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).

Key Words: *Copyright Protection, DCT, Random embedding, Spread Embedding, Watermarking, DWT-SVD, ECC algorithm.*

I. INTRODUCTION

Image watermarking is a technique employed to modify specific pixel values within a digital image for the purpose of embedding copyright information. The goal is to make these embedded copyrights resistant to various manipulations, ensuring that individuals with malicious intent cannot falsely claim ownership of digital images [1]. Image watermarking shares similarities with image steganography, primarily in their function of inserting and concealing data [2]. However, the key distinction lies in their resistance to attacks. Watermarking methods must withstand attacks or image alterations, making them more robust [3] [4]. With advancements in technology, image manipulation techniques have become increasingly sophisticated, necessitating innovative approaches to embed copyright that can resist attacks

ISSN : 2455-9679
SJIF Impact Factor : 6.008

while maintaining visual image quality.

Data insertion methods can be performed in two domains: spatial and frequency domains [5]. In the spatial domain, pixel values within the image are directly modified. While this technique is relatively simpler and results in better image quality, it is more susceptible to image manipulation. In contrast, data insertion in the frequency domain involves complex algorithms and computations but offers greater resistance to various image manipulations.Typically, digital images exist in the spatial domain, and certain calculations are required to transform them into the frequency domain. This transformation process is known as calculation, and the Discrete Cosine Transform (DCT) is one of the most popular and widely used methods, particularly in watermarking techniques [6] [7].

Based on theoretical considerations and testing from previous research, DCT offers several advantages, such as computational speed, a high level of energy compactness, and its standard use in various optical hardware. DCT is a fundamental calculation used in JPEG image compression and MPEG video compression.JPEG is the most commonly used image compression storage format. Research has also demonstrated that DCT is resilient against various attacks and digital image manipulations

While robustness is a crucial aspect of image watermarking, improving the quality of the output image to make the inserted copyright more imperceptible is also essential. One approach to enhance output image quality involves combining DCT algorithms with other transformations, such as wavelets, singular value decomposition, or other methods. Some studies have even combined multiple transformations [9]. However, using multiple transformations can increase algorithm complexity, potentially slowing down computations, especially on low-specification hardware. Another method to enhance output quality is using a spreading technique when embedding copyrights. The PN Sequence can generate random numbers used as guidelines for embedding copyrights. This spread of copyright using PN Sequence across the entire image improves the quality of the watermarked image output .Implementing techniques like these indirectly enhances watermark security .PN generators produce random numbers with relatively simple algorithms, allowing for quick computations when integrated into the watermarking method.

Copyright security is another critical aspect of watermarking. Many contemporary watermarking studies incorporate cryptographic methods to enhance watermark security [11]. Chaotic map-based cryptographic methods are prevalent in current watermarking research [12].However, these methods have limitations as they only randomize pixel values without changing them [13]. In contrast, one-time pad (OTP) cryptography secures watermarks by altering pixel watermark values, a technique widely used in recent watermarking research.OTP cryptography primarily involves the XOR operation. In this research, a novel approach is proposed that combines random technique cryptography and XOR operations to improve the quality of watermarked image output and enhance copyright security.

II. Related Work

Prasanth Vaidya Sanivarapu et.al. 2022[14] Digital images are transferred with ease through the network. Many users are using the images without the knowledge of the owners. Therefore, a novel watermarking scheme is proposed to ensure copyright protection and authentication of images using cryptography techniques. Here, a quick response (QR) image is generated for a watermark image that contains public and private keys prepared using a cryptosystem. Later, this QR image is scrambled using a chaotic logistic map. The public and private keys are used to cipher and decipher the data. Next, the scrambled QR watermark is embedded into a color image using a single-level discrete wavelet transform followed by singular value decomposition using the key value. Finally, the inverse process is applied to extract the watermark. The proposed method is validated using various image processing attacks. The results are then compared with state-of-the-art watermarking schemes. The experimental results show that the scheme provides good results in terms of robustness and imperceptibility.

To handle the above issues, digital watermarking has emerged as an appropriate solution. Digital watermarking is a way of embedding a watermark into a significant image/media. A watermark acts as copyright data, shielding advanced information from illicit replication and conveyance [15]. A watermark is a sort of marker clandestinely inserted in a signal (audio, video, or image information). A watermark embedded into media may or may not relate to it. Watermarks are utilized to check the realness or uprightness of the watermarked signal [16]. Watermarking is a strategy that is broadly utilized and ceaselessly created by utilizing different strategies and executions. In the proposed method, discrete wavelet transform (DWT) and singular value decomposition (SVD) techniques are combined to accomplish the vigor and imperceptibility of the watermark. The scheme is generally achievable for clients and has an oddity edge over

ISSN : 2455-9679
SJIF Impact Factor : 6.008

the other existing digital watermarking methods. The idea of embedding the watermark information is to prevent intruders or other members from claiming to be the rightful owner of the data.

III. PROPOSED WORK

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.

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.

$$\mathbf{A_i = U_i S_i V_i^T}$$

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

$$B_J = U_i S_i V_i^T$$

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 the inverse 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

ISSN : 2455-9679
SJIF Impact Factor : 6.008

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 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

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.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

IV. RESULT & DISCUSSION

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 can be used in order to compute the MSE value, while the formula can be used in order to obtain the PSNR value.

Table 1 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

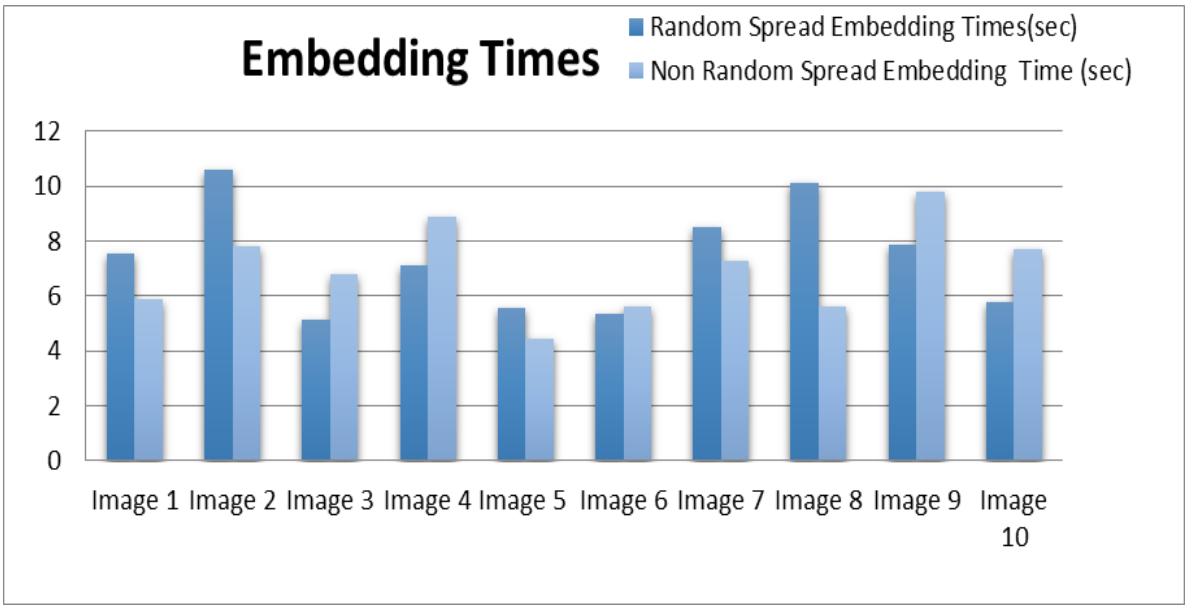

Fig.2 embedding time for random and non random technique

ISSN : 2455-9679
SJIF Impact Factor : 6.008

Table 2 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

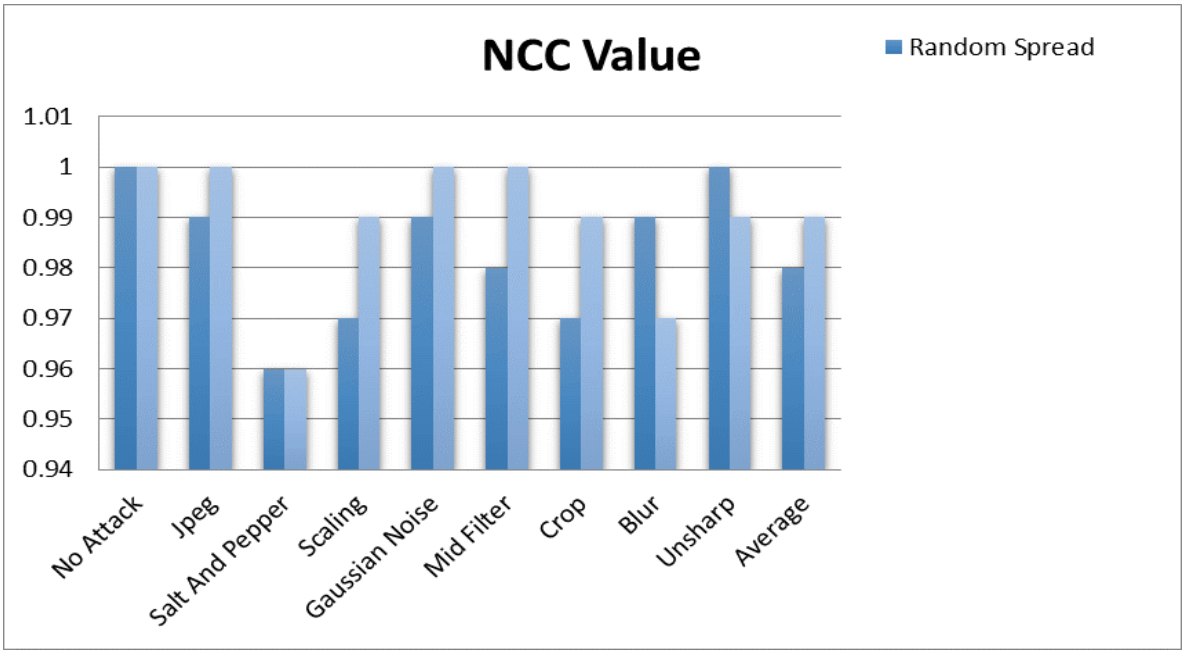

Fig.3 Average of NCC Value from All Images

Table3 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

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. 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

ISSN : 2455-9679
SJIF Impact Factor : 6.008

superior watermarking quality and content security, as evidenced by the higher PSNR value, thereby enhancing the overall effectiveness of digital watermarking and data protection.

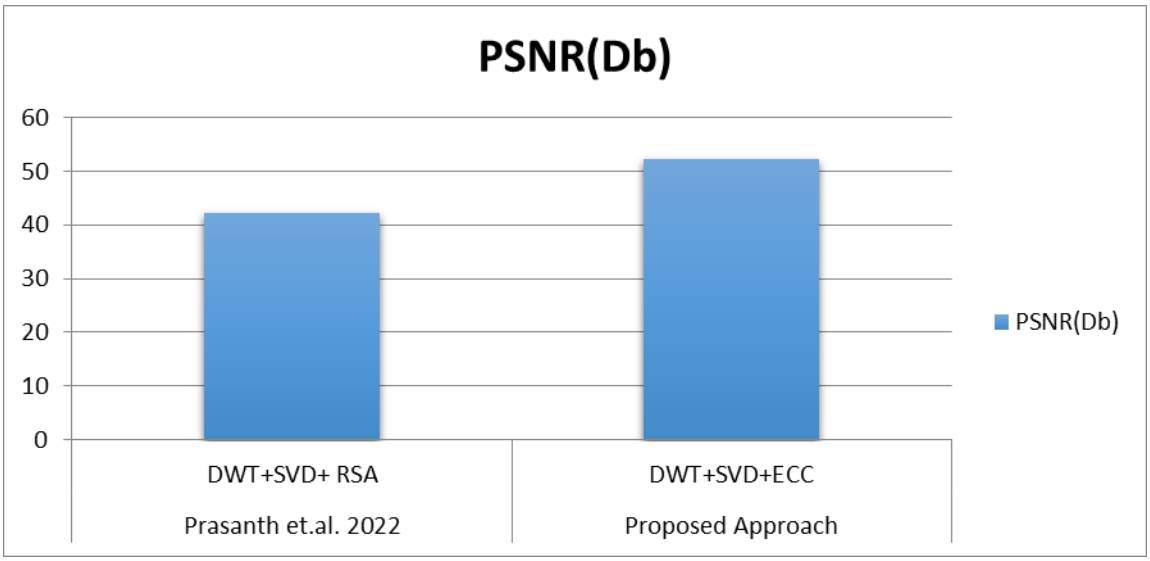

Fig.4 PSNR,MSE,RMSE performance of the proposed approach

V. INTRODUCTION

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.

REFERENCES

[1] Vaidya, S.P. Multiple decompositions-based blind watermarking scheme for color images. In Proceedings of the IEEE International Conference on Recent Trends in Image Processing and Pattern Recognition, Solapur, India, 21–22 December 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 132–143.
[2] Hosny, K.M.; Darwish, M.M. Invariant image watermarking using accurate polar harmonic transforms. Comput. Electr. Eng. 2017, 62, 429–447.
[3] Sanivarapu, P.V.; Rajesh, K.N.V.P.S.; Reddy, N.V.R.; Reddy, N.C.S. Patient data hiding into ECG signal using watermarking in transform domain. Phys. Eng. Sci. Med. 2020, 43, 213–226.
[4] Vaidya, S.P.; PVSSR, C.M. Adaptive digital watermarking for copyright protection of digital images in wavelet domain. Procedia Comput. Sci. 2015, 58, 233–240

[5] Vaidya, P.; PVSSR, C.M. A robust semi-blind watermarking for color images based on multiple decompositions. Multimed. Tools Appl. 2017, 76, 25623–25656.
[6] Hosny, K.M.; Darwish, M.M. Robust color image watermarking using invariant quaternion Legendre-Fourier moments. Multimed. Tools Appl. 2018, 77, 24727–24750.
[7] Vaidya, P.; PVSSR, C.M. Adaptive, robust, and blind digital watermarking using Bhattacharyya distance and bit manipulation. Multimed. Tools Appl. 2018, 77, 5609–5635. 8. Hosny, K.M.; Darwish, M.M.; Fouda, M.M. Robust color images watermarking using new fractional-order exponent moments. IEEE Access 2021, 9, 47425–47435.
[8] Hosny, K.M.; Darwish, M.M.; Li, K.; Salah, A. Parallel multi-core CPU and GPU for fast and robust medical image watermarking. IEEE Access 2018, 6, 77212–77225.
[9] Hosny, K.M.; Darwish, M.M. New geometrically invariant multiple zero watermarking algorithm for color medical images. Biomed. Signal Process. Control 2021, 70, 103007.
[10] Hosny, K.M.; Darwish, M.M. Reversible color image watermarking using fractional-order polar harmonic transforms and a chaotic sine map. Circuits Syst. Signal Process. 2021, 40, 6121–6145.
[11] Samčović, "Robust digital image watermarking based on wavelet transform and spread spectrum techniques," in Telecommunications Forum Telfor, Belgrade, 2015.
[12] A. Ustubioglu, G. Ulutas and M. Ulutas, "DCT based image watermarking method with dynamic gain," in International Conference on Telecommunications and Signal Processing, Prague, 2015.
[13] D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, A. Susanto and M. Doheir, "A Comparative Study of Image Cryptographic Method," in International Conference on Information Technology, Computer and Electrical Engineering, Semarang, 2018.
[14] Prasanth Vaidya Sanivarapu 1 , Kandala N. V. P. S. Rajesh 2 , Khalid M. Hosny 3 and Mostafa M. Fouda 4, Digital Watermarking System for Copyright Protection and Authentication of Images Using Cryptographic Techniques Appl. Sci. 2022, 12, 8724. https://doi.org/10.3390/app12178724
[15] M. Jain and S. K. Lenka, "Secret Data Transmission using Vital Image Steganography over Transposition Cipher," in International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015
[16] A. Setyono, D. R. I. M. Setiadi and Muljono, "StegoCrypt method using wavelet transform and one-time pad for secret image delivery," in International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, 2017.