

Enhanced Robustness Grayscale Image Hybrid Multiple Watermarking Technique and PBVST

Ankit Choubey, Prof. Manish Rai

Research Scholar, Department of CSE

RKDF, RGPV Bhopal, India

ankitchoubey90@gmail.com, manishrai2587@gmail.com

Abstract: - Enhanced robustness grayscale image hybrid multiple watermarking technique and PBVST. The recent time witnessed an excellent need for high-performance digital signal processing (DSP) systems for high end emerging applications, DCT performance low quality. Digital watermarking technology could also be a frontier research field, and it mainly focuses on the property rights, identification and authentication of the digital media to shield the important documents. As indicated by the primary investigation of computerized picture watermarking the advanced watermarking model comprises of two modules, which are watermark implanting module and watermark extraction and discovery module. Digital documents are often copied and scattered easily to large numbers of individuals with none cost. People can download audio, image files, which they will share them with friends which they will influence or change their original contents. Because of this, there's more probability of the copying of such digital information. In this way, there's a critical need of denying such ill-conceived copyright of advanced media. Digital watermarking (DWM) is the dominant solution to this problem. This paper intends to give a thorough investigation of computerized watermarking strategies, mainly centres around advanced picture watermarking DCT and its applications used in numerous the present in the world. It had been upheld the blend of three changes: the discrete wavelet change (DWT), discrete cosine change (DCT) and, the particular worth deterioration (SVD) and mixture numerous watermarking method are low power and low PSNR. During this paper, three watermark pictures of sizes $N \times N$ have picture 512×512 , the viability of the proposed strategy regarding quality and power contrasted with other revealed watermarking methods. Proposed binary values shifting technique supported binary values shifting in image data insert into a cover image in a type of binary values shifting process is proposed approach in this paper which uses the statistical characteristics of the pixels to embed the watermark into improving PSNR values and image watermarking on the Windows platform using Matlab programming language.

Keywords: Digital Watermarking, Frequency Domain, DCT Coefficient, DWT, Attacks, Image Encryption, Image Decryption, Image Recovery, Robustness, PBVST.

I. Introduction

The immeasurable attractiveness of the globe Wide Web in the early 1990s established the commercial potential of offering multimedia resources through digital networks. Since copying a digital data is extremely simple and swift too so, issues like, the shelter of rights of the content and proving ownership, arises. Digital watermarking has been anticipated as one approach to hold out this. Digital watermarking came as a way and a tool to overcome shortcomings of existing copyright laws for digital data. Digital watermarking is a process during which owner identification (watermark) is embedded into the digital media at the sender end and later at the receiver end the embedded information extracted to acknowledge the important owner/identity of the digital content. Digital Image Watermarking is the process of insertion of image watermark in media content and its extraction, if required, for authentication or ownership verification of media content. A digital image watermark may be a piece of data that's hidden directly in media content, in such how that it's invisible to a person's observer [1]. Differing types of watermarking methods for digital contents developed that are classified into different categories depending upon the utilization and therefore, the requirement of data required for the extraction/detection of the watermark to see the authenticity of a digital content fragile watermarking is employed. In contrast, for the aim of copyright protection, robust watermarking is used. This classification is application-dependent. Supported the knowledge required for the extraction/detection process watermarking schemes are often classified into blind, semi-blind, and non-blind categories. Also, another categorization is feasible depending upon the domain of embedding of watermark: spatial and frequency. An in-depth review of watermarking schemes often found in the classifications of earlier developed approaches believe the domain where the key information is going to be embedded and further classified [2].

1.1. Spatial Domain Techniques

In Spatial domain, the watermark directly embedded by modifying the pixels of the first image with none transformation of the image. This system is usually fragile and applied within the pixel domain and has less complex computation, thus consumes less time for archiving and retrieval. The smallest amount significant bit (LSB) technique is employed to embed information during a cover image. The LSB technique of a canopy

image described by changing pixels by bits of the key message. An embedding scheme which randomly hides messages within the LSB of any/all component of the chosen pixel using the polynomial. If a polynomial is employed, the hacker must predict quite one number, i.e. all coefficients of a polynomial have got to be decoded correctly, and the probability of finding alright coefficients is a smaller amount compared to predicting single bit. Watermarking is often done by embedding watermark into sub-images with LSB technique. The watermarks usually embedded into specific blocks of the host image where the choice of blocks predicated on entropy value which provides a high PSNR value. In [8], a unique, robust image watermarking scheme proposed for resisting geometric attacks. Watermark synchronization is first achieved by local invariant regions which may be generated using scale normalization and image feature points. The watermark is embedded in all the local areas repeatedly in the spatial domain. During embedding, each circular region first divided into homocentric cirque regions. Then the watermark bits are embedded by quantizing each cirque region into an odd or even region using odd-even quantization. Within the decoder, an odd-even detector (OED) meant to extract the watermark from the distorted image directly. By utilizing the generating principle and distribution feature of the DC coefficient, a unique blind watermarking algorithm proposed for colour host images in [9]. Firstly, the Y luminance of host image split into 8×8 sub-blocks, and therefore the DC coefficients of every block are directly calculated within the spatial domain. Secondly, consistent with the watermark information and therefore, the quantization step, the DC coefficients are calculated. Their increments further utilized to switch the values of all pixels within the spatial domain directly. When watermark extraction, only the watermarked image and therefore, the quantization step needed within the spatial domain. Low complexity and simple implementation are the benefits of spatial domain watermarking approaches. Despite these benefits, spatial watermarking methods are fragile against image processing operations [3].

1.2. Transformation Domain Techniques

Transformation of a picture is required to urge more information about the image and to scale back the computational complexity. Albeit this system takes longer and more complex than spatial domain technique, the embedded watermarked data can't be identified easily because of the previous technique. In the transform domain, the watermark embedded after performing transformations like Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) etc. The watermark embedded within the transformed coefficients. In comparison to spatial domain techniques, these techniques offer high

security and are robust to attacks. In the frequency domain watermarking, the values of selected frequencies often altered. Since high frequencies are going to be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies containing important elements of the first picture [4]. DCT based image watermarking is more robust as compared to the spatial domain watermarking techniques. DCT may be a fast transformation technique provides excellent energy compaction for highly correlated data, and most of the knowledge (DC coefficient) is within the first pixel. Proposes a robust watermarking approach supported the Discrete Cosine Transform (DCT) domain that mixes Quick Response (QR) Code and chaotic system. When embedding the watermark, the high error correction performance and therefore, the strong decoding capabilities of QR Code are utilized to decode the text watermark information which improves the robustness of the watermarking algorithm. Then the QR Code image is encrypted with a chaotic system to reinforce the protection of this approach. Finally, the encrypted image is embedded to the carrier image's DCT blocks after they underwent block-based Arnold scrambling transformation. During the extraction process, as long because the QR Code image often decoded, the completeness and accuracy of the text watermarking information are usually guaranteed. In a replacement DCT based additive watermarking scheme was proposed which provides higher resistance to image processing attacks mainly JPEG compression. During this approach, the watermark embedded within the mid waveband of the DCT blocks only within the sub-band, which is carrying low-frequency components and therefore the high-frequency sub-band components remain untouched. A DCT based image watermarking framework proposed to reinforce the robustness of the watermark within the watermarked image against high-level lossy JPEG compression.

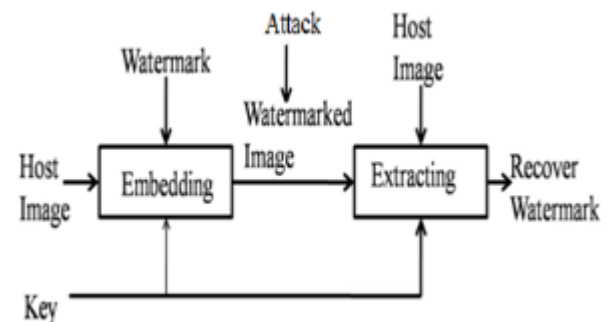


Fig1. General block diagram of embedding and extracting process of digital watermarking

Several proposed watermark frameworks in a previous couple of years have considered binary watermarks and watermark pixels directly embedded at the DCT coefficients of host images. Whereas during this

framework used colour host images and grayscale watermarks and DCT performed on both the host image and watermark image. Watermark frequencies embedded within the DCT coefficients of several blocks of the host image. A secret key's used that determines the embedding blocks of the host image [5].

II. Related Work

Srivastava et al. [6] Digital image watermarking are hiding information in any form (text, image, audio and video) in the original image without degrading its perceptual quality, which predicated on the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) by using Arnold Transform method. DCT based watermarking techniques offers compression while DWT based compression offers scalability. Thus of these desirable properties are often utilized to make a replacement robust watermarking technique. The DCT coefficients of the DWT coefficients are wont to embed the watermarking information. So we choose SVD based digital watermarking which may be a method of authentication data embedding in image characteristics with the expectation to point out resiliency against different kind of unintentional or deliberate attacks. Here discrete wavelet transform plays the important role of an efficient tool because of its multi-resolution capability. Alongside this wavelet transform, we error another powerful mathematical tool called the singular value decomposition (SVD). Though till date, both of them have individually been used as a tool for watermarking of digital media, only a few works have utilized their skills in tandem, especially during this area. Our work now focuses on using Direction Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) by employing a hybrid technology developed for the cover of the property with better robustness against the favoured malicious attacks. Thus we've seen practically by attacking the watermarked image against simulated attacks and recovering the brand from it.

Imran et al. [7] Digital Watermarking is an emerging field that aims to increase the advantages of authentication and copyright to digital media. These Watermarks remain hidden and don't degrade the standard of digital media. Different techniques used for incorporating watermarks into the media. Similar techniques are used at the receiver to retrieve watermarks. However, watermarks are vulnerable to attacks, and robustness, which quantifies the resilience to attacks, is a crucial property for all watermarks. However, in most cases, it's the appliance, that the watermarking is employed, that dictates the features that watermark should possess. During this paper, we've elucidated the techniques and applications of digital watermarking.

Patel et al. [8] because of the recent progress in the internet, digital contents, e.g. video, audio, images are widely used. Protection of digital contents must require. So, it's become a challenging task to guard the copyright of a person's creation. Digital Image Watermarking aims to make sure and facilitate data authentication, security and copyright protection of digital images. This paper elaborates watermarking overview, embedding techniques, watermarking attacks, performance analysis. It'll be useful for researchers to implement compelling image watermarking technique

Kaur et al. [9] this paper presents the challenges for a strong digital image watermarking algorithm. Need for copyright protection in digital media has led to enormous growth within the field of Digital Image Watermarking, whereby researchers are striving to return up with new ways of content protection. Recent developments within the field of watermarking though have provided new ways of protecting data yet there are many factors which require to be addressed such the algorithm of embedding/ extracting a watermark is strong enough to satisfy these challenges. Robustness is often defined as resilience for a watermark to stay unaffected even when digital content is skilled in various processes and attacks and hence increase security, capacity, and imperceptibility of watermarked data. The paper begins with a quick introduction to cryptography and Steganography, which is the platform for a variety of digital watermarking concepts. Then, requirements for watermarking systems discussed alongside methods to watermark data efficiently and their strengths and weaknesses. Last, there's a replacement method proposed which uses an idea of nested watermarks using Discrete Wavelet Transform for binary images and Cryptography using Spread Spectrum technique and meant to be robust enough to cater to challenges presented here.

Jabade et al. [10] in image watermarking, information is embedded into cover media to prove ownership. Various watermarking techniques are proposed by many authors within the last several years, which include spatial domain and transform domain watermarking. Wavelet-based image watermarking is gaining more popularity due to its resemblance to the human sensory system. This paper elaborates suitability of wavelet transform for image watermarking; wavelet transform based image watermarking process, classification and analysis of wavelet-based watermarking techniques. This paper aims to supply a comprehensive review of the prevailing literature available on wavelet-based image watermarking methods. It'll be useful for researchers to implement effective image watermarking method.

Yeung et al. [11] they propose a replacement method for invisibly watermarking high-quality colour and grayscale

images. This method meant to be used in image verification applications, where one is curious about knowing whether the content of a picture has been altered since some earlier time, perhaps due to the act of a malicious party. It consists of both a watermark stamping process which embeds a watermark during a source image and a watermark extraction process which extracts a watermark from a stamped image. The extracted watermark is often wont to determine whether the image has been altered. The processing utilized in the stamping and extraction processes presented. We also discuss some advantages of this system over other invisible watermarking techniques for the verification application; these include a high degree of invisibility, colour preservation, simple decoding, and a high degree of protection against retention of the watermark after unauthorized alterations.

Hussein et al. [12] Digital watermarking techniques developed to shield the copyright of digital media. This paper aims to supply an in-depth review and background about the watermarking definition, concept and therefore, the main contributions during this field. It begins with a digital watermarking overview, general framework, attacks, application, and eventually, a comprehensive survey of existing and most up-to-date watermarking techniques. We classify the methods according to various categories like host signal, perceptivity, robustness, watermark type, necessary data for extraction, processing domain, and applications. Within the survey, our main concern is an image only.

Li et al. [13] Watermark robustness to geometric attacks remains a challenging research field. During this paper, a unique, robust image watermarking scheme proposed for resisting such attacks. Watermark synchronization is first achieved by local invariant regions which may be generated using scale normalization and image feature points. The watermark is embedded into all the local regions repeatedly in the spatial domain. During embedding, each circular region first divided into homocentric cirque regions. Then the watermark bits are embedded by quantizing each cirque region into an "odd" or "even" region using odd-even quantization. Within the decoder, an odd-even detector (OED) meant to extract the watermark from the distorted image directly. Localized embedding achieves good invisibility, and repeated insertion enhances watermark robustness. Simulation results show that the proposed scheme is strong to both geometric attacks and traditional signal processing attacks.

Lang et al. [14] proposed a unique blind digital image watermarking algorithm supported the fractional Fourier transform (FRFT), which may be a generalization of the standard Fourier transform and its output has the mixed time and frequency components of the signal. The

first image segmented into non-overlapping blocks for watermarking, and every block is transformed by the two dimensional fractional Fourier transform with two fractional orders. Then each pixel value of binary watermark is embedded by modifying the back-diagonal FRFT coefficients of every image block at an equivalent location with a random array. After performing an inverse two dimensional fractional Fourier transform, we will obtain the watermarked image, and therefore, the transform orders often considered because of the encryption keys during this method. A series of attacking experiments performed on the proposed method. The experiments results show that the proposed algorithm not only is of excellent imperceptibility and security and is exceptionally robust to JPEG compression noise attacks and image manipulation operations but can also provide protection even under compound attack.

Chang et al. [15]. Within the past few years, several digital watermarking schemes are proposed and supported DCT, DFT, and DWT transformations. During this paper, singular value decomposition (SVD)-based watermarking scheme proposed. SVD transformation preserves both one-way and non-symmetric properties, usually not obtainable in DCT and DFT transformations. Within the proposed method, both of the D and U components explored for embedding the watermark. Experimental results show that the standard of the watermarked image is good, which there strong resistance against general image processing is. Furthermore, the extracted watermark can still be easily identified after tampering.

III. MATLAB Tool

It is simulating on Matlab programming language, and for this work, we use Intel 2.4 GHz Machine. Matlab programming language setup may be a high-level language, and technical calculate and interactive surroundings for algorithmic program development, information visualization, records analysis, and numeric computation Matlab programming language might be a product framework program that grants you to attempt to data control and representation, computations, science and programming. It is wont to do easily moreover as terribly subtle tasks. Image procedure function provides a comprehensive set of reference usual method graphical tools for image process, analysis, visualization, and algorithmic program development. You'll be able to perform image improvement, image declaring, feature detection, noise decrease, image segmentation, abstraction transformations, and image registration. A few capacities inside the device case are multithreaded to require beneficial thing about multicore and advanced PC PCs. The Performance analysis of Matlab programming language, i.e. used for these thesis simulation results of image process provides processor optimized libraries for quick execution and

image computation. It utilizes its JIT (without a moment to spare) accumulation innovation to create execution speeds that rival antiquated programming dialects. It might likewise more preferred position of multicenter and advanced PC PCs, Matlab programming language gives a few multi-rib variables based math and mathematical perform. These functions mechanically execute on multiple procedure thread during a single Matlab programming language session, enabling them to execute quicker on multicore computers. During this thesis, all increased pictures results were performed in Matlab programming language to induce AN increased results of the compressed and decompressed image, and once colourization of the decompressed image, image quality and numerical price once analysis. To check the planned technique, Simulation victimization Matlab programming language is performed on input pictures. The simulation tool is that the language and interactive environment utilized by many engineers and scientists worldwide. It lets explore and visualize ideas and collaborate across entirely different disciplines with signal and image process, communication and computation of results. Matlab programming language provides tools to accumulate, analyze, and visualize information, change you to achieve insight into your information during a fraction of the time it might take mistreatment spreadsheets or ancient programming languages. It may also document and share the results through plots and reports or as revealed Matlab programming language code. The simulation tool is a content matrix laboratory may be a numerical computing and multi-paradigm scenario and fourth-generation programming language. It's developed by mathematics work; Matlab programming language permits matrix strategy, plotting of performing and information, implementation of the algorithmic program, construction of user interfaces and interfacing with programs.

IV. Result Analysis

The main objective of Digital watermark Robustness: The watermark should be ready to withstand after normal signal processing operations like image data secure transformation. Imperceptibility: The watermarked image should appear as if the same because the original image to the traditional eye. The viewer cannot detect that watermark is embedded in it and eventually improve PSNR.

(a) Experimental 1: Butterfly covers image and Google-plus logo data image: Analysis on-base PSNR and NC: Google-plus logo (64x64, 1.52KB) as a data image and butterfly (512x512, 291 KB) as a cover image are both embedding and obtain the watermarked image. In case of noise attack analysis on base PSNR and NC, PBVST process evaluation of PSNR value is high, HWT process evaluation of PSNR value is low. In show fig2.

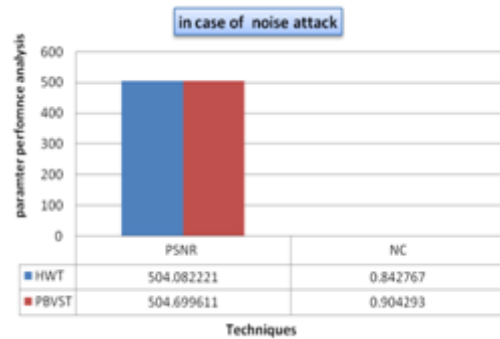


Figure Experimental 1: Analysis between PSNR and NC

Google-plus logo (64x64, 1.52KB) as a data image and butterfly (512x512, 291 KB) as a cover image are both embedding and obtain the watermarked image. In case of noise attack analysis on base ET and RT, PBVST process evaluation of ET and RT is less, HWT process evaluation of ET and RT are average. In show fig3.

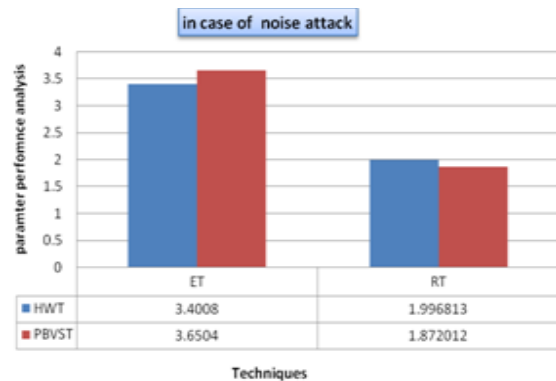


Figure 3 Experimental 1: Analysis between ET and RT

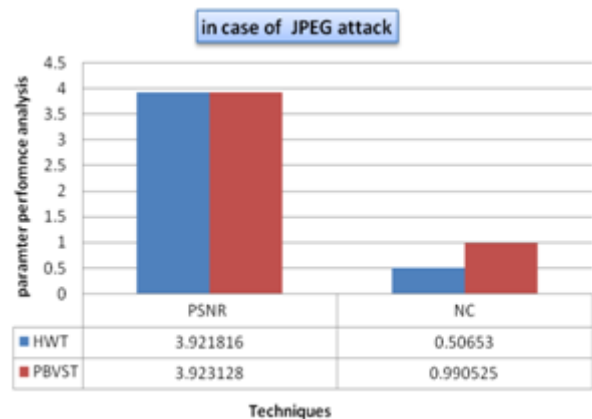


Figure 4 Experimental 2: Analysis between PSNR and NC

(b) Experimental 1: rkdf_word message (64x64, 574 Bytes) as a data image and couple_image (512x512, 257 KB) as a cover image are both embedding and obtain the watermarked image. In case JPEG attack analysis on base PSNR and NC, PBVST process evaluation of PSNR value is high, HWT process evaluation of PSNR value is low. In show figure 4. Rkdf_word message (64x64, 574 Bytes) as a data image and couple_image (512x512, 257 KB) as a

cover image are both embedding and obtain the watermarked image. In case JPEG attack analysis on base ET and RT, PBVST process evaluation of ET and RT is less, HWT process evaluation of ET and RT are average. In show fig5.

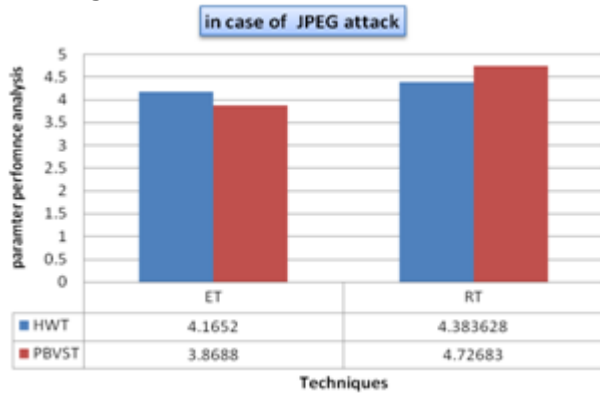


Figure 5 Experimental 2: Analysis between ET and RT

V. Conclusion

Enhanced robustness grayscale image hybrid multiple watermarking techniques and proposed binary values shifting technique (PBVST). Proposed binary values are shifting technique based on digital image watermarking approaches and one-bit position the watermark within the digital image just in case of space shortage problem. In recent years digital watermarking has achieved great deal attention. Distribution of images is now faster and more accessible via technology, especially on the web. They were concerned about illegal copying of their content. Watermarking techniques and hybrid, multiple watermarking techniques are standard image data or multimedia security on internet data transmission time. Watermarking DCT doesn't provide permanent protection, but it does not provide robustness, invisibility, data capacity and security. They need to offer various aspects of digital image watermarking in terms of overview, watermarking techniques, attacks, applications, performance analysis. Aside from it, a quick and comparative investigation of watermarking techniques presented. It's concluded that the prevailing systems often improvised to supply an error-resilient DCT architecture to compare other proposed method the overall architecture and to design, implement and validate DCT architecture and watermarking techniques using different standards image processing parameter. During this paper, they study the previous existing DCT approaches and that they found there are many issues which are associated with algorithm & architecture level. So during this area, there's many our proposed method where they will still make many improvements. Proposed binary values shifting technique (PBVST) improve PSNR values and also improve robustness in image watermarking against attack, the Windows platform using Matlab programming language.

References

- [1]. Jo, Minho, and HyoungDo Kim. "A digital image watermarking scheme based on vector quantization." *IEICE Transactions on Information and Systems* 85, no. 6 (2002): 1054-1056.
- [2]. Liu, Yang, Shanyu Tang, Ran Liu, Liping Zhang, and Zhao Ma. "Secure and robust digital image watermarking scheme using logistic and RSA encryption." *Expert Systems with Applications* 97 (2018): 95-105.
- [3]. Nikolaidis, Nikos, and Ioannis Pitas. "Robust image watermarking in the spatial domain." *Signal processing* 66, no. 3 (1998): 385-403.
- [4]. Ratnakar, Viresh, Victor Ivashin, and Vasudev Bhaskaran. "Image transformations in the compressed domain." U.S. Patent 6,298,166, issued October 2, 2001.
- [5]. Jiansheng, Mei, Li Sukang, and Tan Xiaomei. "A digital watermarking algorithm based on DCT and DWT." In *Proceedings. The 2009 International Symposium on Web Information Systems and Applications (WISA 2009)*, p. 104. Academy Publisher, 2009.
- [6]. Saqib, Manasha, and Sameena Naaz. "Spatial and frequency domain digital image watermarking techniques for copyright protection." *Int. J. Eng. Sci. Technol* 9: 691-699, 2017.
- [7]. Tsai, Min-Jen, Kuang-Yao Yu, and Yi-Zhang Chen. "Joint wavelet and spatial transformation for digital watermarking." *IEEE Transactions on Consumer Electronics* 46, no. 1: 237, 2000.
- [8]. Santhi, V., and Pachiyappan Arulmozhivarman. "Hadamard transform based adaptive visible/invisible watermarking scheme for digital images." *Journal of Information Security and Applications* 18, no. 4: 167-179, 2013.
- [9]. Podilchuk, Christine I., and Edward J. Delp. "Digital watermarking: algorithms and applications." *IEEE signal processing Magazine* 18, no. 4: 33-46, 2001.
- [10]. Moskowitz, Scott A. "Multiple transform utilization and application for secure digital watermarking." U.S. Patent 7,738,659, issued June 15, 2010.
- [11]. Srivastava, Shubham, and Arun Kumar. "Image Enhancement in Digital Image Watermarking Using Hybrid Image Transformation Techniques." *IOSR Journal of Electronics and Communication Engineering*, ISSN: 2278-8735. Volume 11, Issue 3, Ver. II, PP 116-121, June 2016.

- [12]. Imran, Sheikh, Ravinder Chaudhry, Junaid Gilani, and Suhail Nehvi. "The Techniques and Applications of Digital Watermarking." 2014.
- [13]. Patel, Jalpa M., and Prayag Patel. "A brief survey of digital image watermarking techniques." *International Journal for Technological Research in Engineering* 1, no. 7, 2014.
- [14]. Kaur, Deepti Prit, Jaspreet Kaur, and Kamal Deep. "Digital image watermarking: Challenges and approach for a robust algorithm." *International Journal of Electronics Engineering* 1, no. 1 95-97, 2009.
- [15]. Jabade, Vaishali S., and Dr Sachin R. Gengaje. "Literature review of wavelet-based digital image watermarking techniques." *International Journal of Computer Applications* 31, no. 1: 28-35, 2011.
- [16]. Yeung, Minerva M., and Fred Mintzer. "An invisible watermarking technique for image verification." In *Proceedings of the international conference on image processing*, vol. 2, pp. 680-683. IEEE, 1997.
- [17]. Hussein, Ensaf, and Mohamed A. Belal. "Digital watermarking techniques, applications and attacks applied to digital media: a survey." *threshold* 5: 6, 2012.
- [18]. Li, Lei-Da, and Bao-Long Guo. "Localized image watermarking in the spatial domain resistant to geometric attacks." *AEU-International Journal of Electronics and Communications* 63, no. 2: 123-131, 2009.
- [19]. Lang, Jun, and Zheng-Guang Zhang. "Blind digital watermarking method in the fractional Fourier transform domain." *Optics and Lasers in Engineering* 53: 112-121, 2014.
- [20]. Chang, Chin-Chen, Piyu Tsai, and Chia-Chen Lin. "SVD-based digital image watermarking scheme." *Pattern Recognition Letters* 26, no. 10: 1577-1586, 2005.
- [21]. Bangaleea, R., and H. C. S. Rughooputh. "Performance improvement of spread spectrum spatial-domain watermarking scheme through diversity and attack characterization." In *IEEE AFRICAN. 6th African Conference in Africa*, vol. 1, pp. 293-298. IEEE, 2002.
- [22]. Larijani, Houtan Haddad, and Gholamali Rezai Rad. "A new spatial domain algorithm for grayscale images watermarking." In *2008 International Conference on Computer and Communication Engineering*, pp. 157-161. IEEE, 2008.