Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 3 (2024)

A Novel Approach to Achieve Dual Security in Images Using Advanced Watermarking Technique

[1]Kiran Pithiya, [2]Khyati Zalawadia , [3]Ashish Kothari

[1] Department of Computer Applications, Faculty of Science, MSU, Vadodara
[2] Computer Science and Engineering dept , PIET, Parul University Vadodara, India
[3] Aatmiya University , Rajkot, India

Abstract:- As the digital landscape continues to evolve, the need for robust security measures to protect digital assets, particularly images, has become increasingly paramount. This research paper introduces a novel approach to achieve dual security in images through the integration of advanced watermarking techniques. By combining visible and invisible watermarks in multiple domains and incorporating dynamic elements, this approach aims to enhance image security, discouraging unauthorized use and ensuring the integrity of digital content.

Keywords*:* Dual Security, Digital watermarking, Correlation-based invisible watermarking

1. I Introduction

In the digital era, where images play a pivotal role in communication, creativity, and information sharing, ensuring the security of these visual assets has become a paramount concern. The proliferation of digital content across diverse platforms and the ease of accessibility have amplified the risk of unauthorized use, tampering, and infringement. As a response to these challenges, the concept of dual security in images has emerged as a sophisticated and comprehensive approach to safeguarding digital visual data.

Traditional security measures often rely on a singular layer of protection, leaving vulnerabilities that can be exploited by determined attackers. Dual security, as applied to images, introduces a multifaceted defense mechanism that combines the strengths of different security layers, significantly enhancing the overall resilience of the system. This approach goes beyond conventional methods and aims to address the evolving threats and complexities associated with the digital landscape.

The core idea behind dual security in images involves the integration of two distinct but complementary levels of protection. This typically encompasses the deployment of both visible and invisible watermarks, strategically embedded within the image data. Visible watermarks act as a deterrent, providing a clear and overt indication of ownership or copyright, while invisible watermarks operate discreetly, imperceptible to the human eye but detectable through specialized algorithms. The synergy of these two types of watermarks creates a robust defense against unauthorized use, manipulation, or duplication.

With the advent of advanced watermarking techniques, researchers and practitioners are exploring innovative strategies to fortify the security of digital images. This includes incorporating multi-domain watermarking, dynamic watermarking that adapts over time, key-based approaches for secure embedding and extraction, and the fusion of watermarks for added complexity. These advancements aim to create a dual security paradigm that not only protects against common attacks like compression and cropping but also ensures authentication and authorization in the extraction process.

The importance of dual security in images extends beyond mere protection; it in stills confidence in content creators, facilitates trustworthy information dissemination, and fosters a secure digital environment. In this era

of rapid digital transformation, understanding and implementing dual security measures in images become imperative for individuals, businesses, and organizations seeking to preserve the integrity, ownership, and authenticity of their visual assets. As we delve deeper into the nuances of dual security in images, this exploration will uncover innovative methodologies, challenges, and future directions in the pursuit of a more secure and reliable digital visual landscape.

- Provide an overview of the current challenges in image security.
- Highlight the significance of dual security for safeguarding digital images.
- Introduce the concept of watermarking as a method for securing digital content.

2. Literature Review

Dual security in images involves highlighting key works that contribute to the understanding and development of this concept. Here's a reference summary with notable works in the field:

Cox, I.J., Miller, M.L., and Bloom, J.A. (2002).provide a comprehensive overview of digital watermarking techniques, including both visible and invisible methods. It serves as a key reference for understanding the basics of watermarking in the context of image security [1].

Barni, M., and Bartolini, F. (2005) also works on Enabling Digital Assets Security and Other Applications. Focusing on engineering aspects, this work explores the design and implementation of watermarking systems. It discusses key engineering principles and strategies for achieving robust security in digital images[2].

Cox, I.J., Kilian, J., Leighton, T., and Shamoon, T. (1997) derived and developed Spread Spectrum based Watermarking for Multimedia. This seminal paper introduces the concept of spread spectrum watermarking, a technique widely used in invisible watermarking. The paper discusses how spread spectrum methods enhance robustnss against various attacks[3].

This book provides an in-depth exploration of digital watermarking algorithms and their applications. It covers various domains, including images, and is valuable for understanding the technical intricacies of watermarking.[Podilchuk, C.I., and Delp, E.J. (2001). Digital Watermarking: Algorithms and Applications [4].

This work addresses the crucial aspect of robustness in watermarking. It discusses techniques for ensuring that watermarks remain intact under various attacks, contributing to the development of resilient dual security systems.Swaminathan, A., Mao, Y., and Wu, M. (2006). Robust and Imperceptible Watermarking of Images.[5]

Exploring reversible watermarking, this paper introduces a method based on the difference expansion of triplets. It contributes to discussions on reversible techniques, which are essential for maintaining the quality of watermarked images. Alattar, A.M. (2005). Reversible Watermark using the Difference Expansion of Triplets.[6]

Zhang, X., Li, X., and Zhao, H. (2016).. This paper proposes a dual watermarking algorithm that operates in multiple domains, showcasing the importance of multi-domain approaches for achieving robust dual security [7]

Piva, A., Barni, M., and Bartolini, F. (2003), focused on Addressing the issue of integrity control, this work introduces a watermarking-based approach for verifying the authenticity of digital images, contributing to the broader understanding of image security.[8]

This paper introduces a hybrid and blind watermarking scheme operating in the DCuT–RDWT domain. By combining the discrete curvelet transform (DCuT) and redundant discrete wavelet transform (RDWT), the scheme aims to enhance imperceptibility. The emphasis is on blind watermarking methods. [9]

This paper presents a multi-level security approach for medical images in telemedicine, incorporating both encryption and watermarking techniques. The emphasis on multi-level security underscores the significance of safeguarding sensitive medical data.[10]

This paper introduces a hybrid domain watermarking technique for image copyright protection, employing speech watermarks. The hybrid approach likely combines different signal processing transforms to enhance invisibility and robustness. The use of speech watermarks introduces a novel and potentially secure element to the copyright protection strategy.[11]

Christine I. Podilchukand Raymond B. Wolfgang [1] described the invisible but transparent watermarking scheme for image as well as video. They explained the exploitation of properties of human visual system. They explained the concepts of image and video watermarking using DCT and modification of the frequency coefficients. They also described that more work is required to be performed to make this scheme more robust. They specifically pointed this sentence towards the video watermarking.

G. C. Langelaar, I.Setyawan and Reginald L. Lagendijk [2] beautifully reviewed the current watermarking techniques, need of watermarking, application of watermarking and requirement of watermarking algorithms. The authors lightened a lamp on algorithms that has already been implied in spatial and frequency domain. The authors lighted a lamp on what methods and what mathematical expressions are used for changing the pixel value according to the watermark in the spatial as well as in the transform domain. The authors also stated the methods used for image and video. They also given the idea of properties of the human visual system.

Podilchuk, C.I. and Delp, E.J. [3] given the idea of what has already been done in the field of watermarking. They explained concepts of digital watermarking. They lighten the lamp on how various multimedia can be watermarked. They covered the concepts of image, audio, video and graphics watermarking. They also highlighted the work that should be done in the field of watermarking by stating the limitations of the current methods.

R. Chandramouli, N. D. Memon, and M. Rabbani [4] explained various concepts of digital watermarking. They beautifully highlighted the types of watermarking, applications where digital watermarking may be used, the requirement of watermarking and difference between the steganography and watermarking.

From above summary encompasses key works that cover various aspects of dual security in images, including watermarking techniques, robustness, key-based approaches, and novel strategies for enhancing image protection.

- Existing watermarking techniques and their applications in image security.

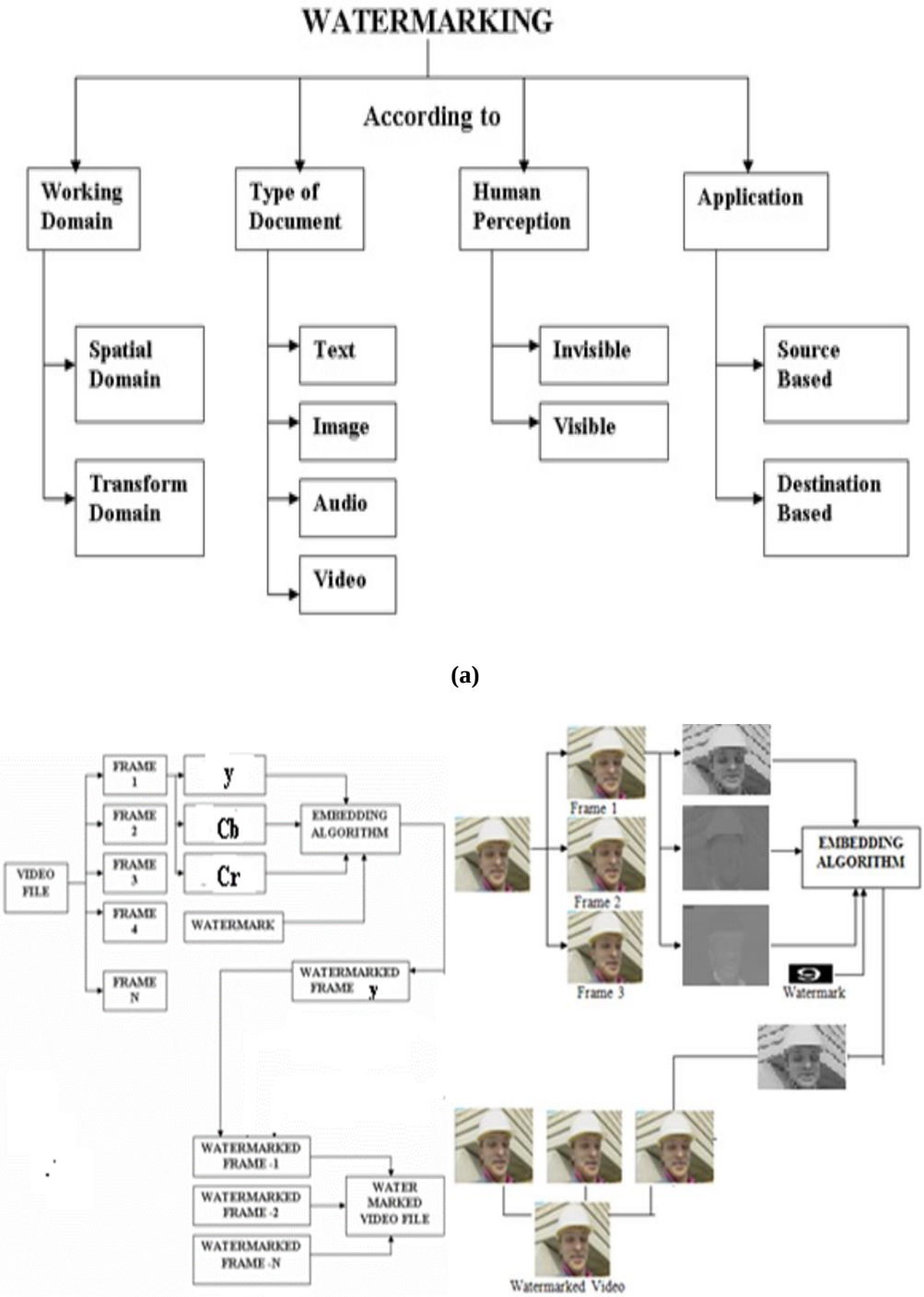


Figure 1 (a) Water Marking Scheme (b) General Idea of Digital Watermarking (c) Implementation of

Where, y – Luminance Component – Very Important and Informative Cb and Cr – Less Informative and Less Important
Y is used for watermarking purpose because HVS is sensitive more towards **brightness** compare to color.

3. Types of Watermarking

In the dynamic landscape of digital media, the security of images is a critical concern. The proliferation of image-based communication and the ease of digital content distribution have elevated the risks associated with

unauthorized use, manipulation, and piracy. Traditional security measures, often singular in nature, are no longer sufficient to thwart the diverse and sophisticated threats faced by digital images. In response, the concept of dual security in images has emerged as a comprehensive and innovative approach to fortify the protection of digital visual assets.

1. Visible and Invisible Watermarking:

Dual security in images involves the integration of both visible and invisible watermarks. Visible watermarks serve as a deterrent, acting as a conspicuous marker that indicates ownership or copyright information. On the other hand, invisible watermarks are embedded within the image data using advanced techniques, remaining imperceptible to the human eye but detectable through specialized algorithms. This dual-layered watermarking strategy creates a robust defence against unauthorized use and manipulation.

2. Multi-Domain Watermarking:

To enhance the overall resilience of the security system, multi-domain watermarking is often employed. Watermarks can be embedded in various domains, including spatial, frequency, and color spaces. This multi-dimensional approach makes it more challenging for potential attackers to remove or alter watermarks without affecting the image's integrity.

3. Dynamic Watermarking:

Dynamic watermarking introduces an element of adaptability to the security framework. Rather than employing static watermarks, dynamic watermarking involves altering the watermark properties over time. This not only increases the system's resistance to attacks but also ensures the longevity and relevance of the security measures in an ever-changing digital landscape.

4. Key-Based Security:

A key-based approach adds an extra layer of security by incorporating secret keys during the watermarking process. This ensures that only authorized parties with the correct keys can extract, verify, and modify the watermarks. Key-based security provides an effective means of controlling access to sensitive image data.

5. Fusion of Watermarks:

The fusion of visible and invisible watermarks is explored to create a more intricate and resilient security system. By combining these two types of watermarks in a complementary manner, the dual security approach becomes more robust, making it challenging for adversaries to compromise both layers simultaneously.

6. Authentication and Authorization:

Authentication and authorization mechanisms play a crucial role in dual security. Secure key management, encryption, and access control are implemented to verify the legitimacy of users attempting to extract or modify watermarks. This ensures that only authorized individuals can access and manipulate the protected images.

Dual security systems may face challenges in maintaining robustness against emerging attacks and sophisticated manipulation techniques. Adversaries may exploit vulnerabilities in watermarking methods, reducing the overall effectiveness of the security measures.

The incorporation of both visible and invisible watermarks is fundamental to achieving dual security in digital images. Each type of watermark serves a distinct purpose, contributing to a comprehensive security strategy that aims to deter unauthorized use, identify ownership, and resist tampering.

4. Importance of Watermarking with Dual Security

1. Deterrence and Ownership Identification:

Visible Watermarks:

Visible watermarks act as a visual deterrent, signaling to users that the image is protected and carries ownership or copyright information. They are easily recognizable and discourage unauthorized use by making it clear that the content is the intellectual property of someone else.

Role in Dual Security: The presence of a visible watermark serves as a first line of defense, dissuading potential infringers and enhancing the perception of ownership rights. Even if an image undergoes modifications, the visible watermark can often survive, maintaining a clear link to the original creator or owner.

2. Stealth and Tamper Resistance:

Invisible Watermarks:

Invisible watermarks, also known as digital watermarks, are embedded within the image without being perceptible to the human eye. They provide a covert layer of security, allowing for the identification and authentication of the image without altering its visual appearance.

Role in Dual Security: Invisible watermarks play a crucial role in securing images discreetly. Even if an infringer attempts to remove or modify visible watermarks, the invisible watermark remains intact, providing an additional and less obvious layer of protection. This covert feature enhances the overall resistance to tampering.

3. Resilience and Redundancy:

The combination of both types of watermarks introduces redundancy, ensuring that even if one layer is compromised, the other may still provide a level of security. This redundancy enhances the overall resilience of the dual security system.

Role in Dual Security: Visible and invisible watermarks complement each other. While visible watermarks act as a deterrent and are often easier to remove, invisible watermarks offer a more robust and covert means of identification. The fusion of these two approaches creates a dual security system that is more challenging for attackers to circumvent successfully.

4. User Perception and Trust:

Visible watermarks are crucial for shaping user perceptions and building trust. Users are more likely to recognize and respect ownership rights when they see a visible watermark, which, in turn, fosters trust in the authenticity of the content.

Role in Dual Security: The presence of both visible and invisible watermarks enhances user confidence. While visible watermarks establish immediate recognition of ownership, invisible watermarks add an additional layer of assurance, assuring users that the content is not only visibly protected but also digitally authenticated.

5. Legal and Forensic Implications:

Visible watermarks often carry copyright information and serve as a clear legal statement of ownership. Meanwhile, invisible watermarks provide a forensic trail that can be crucial in legal proceedings to prove ownership and authenticity.

Role in Dual Security: The combination of visible and invisible watermarks reinforces the legal standing of the content owner. Visible watermarks provide a public assertion of ownership, while invisible watermarks offer a more discreet and technical means of proving authenticity when legal challenges arise.

the importance of visible and invisible watermarks in achieving dual security lies in their complementary roles. Visible watermarks act as a visible deterrent and ownership identifier, while invisible watermarks provide a covert, tamper-resistant layer that enhances overall security. The synergy between these two types of watermarks creates a robust dual security system that addresses different aspects of image protection and authentication.

5. Proposed Approach

Invisible watermarking is a technique used to embed information into digital media, such as images, audio, or video, without perceptibly altering the original content. The correlation-based method is one approach to achieve this. In this method, the watermark is embedded by modifying the original data in a way that its correlation with the embedded watermark can be detected later.

Here is a basic equation representing the correlation-based invisible watermarking process:

1. Embedding Process

Let $I(x,y)$ be the original image, and $W(x,y)$ be the watermark image. The watermark is embedded into the original image using a correlation-based method. One common method is to add a scaled version of the watermark to the original image.

The watermarked image $Iw(x,y)$ can be expressed as:

$$Iw(x,y)=I(x,y)+\alpha \cdot W(x,y)$$

Where α is a scaling factor that controls the strength of the watermark.

2. Detection Process

After the watermark has been embedded, it can be detected using correlation. The correlation function $C(x,y)$ between the watermarked image and the original watermark can be computed as:

$$C(x,y)=\sum i,jIw(x+i,y+j)\cdot W(i,j)$$

A higher correlation value indicates a stronger presence of the watermark. By comparing the correlation values at different locations, the watermark can be detected.

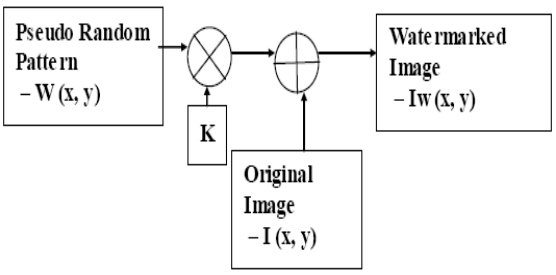


Figure 2 . Two Processes – one for watermark bit 0 and the other for bit 1

It's important to note that the actual implementation of invisible watermarking involves additional considerations, such as normalization, error correction, and robustness against common image processing operations. The choice of the scaling factor α and other parameters depends on the specific requirements of the application and the desired trade-off between watermark visibility and robustness. Additionally, this is a simplified representation, and real-world implementations may involve more sophisticated techniques and considerations for security and reliability.

6. Output of Extraction Process

Figure 3. Embedding Process – Results Gain factor-100

Extraction Process step by step

- Use the same PN sequences

- Find the correlation of the block of the frame with both PN sequence.
- If Correlation with PN sequence zero is higher than that with PN sequence one assign recovered bit to be 0 otherwise assign 1.

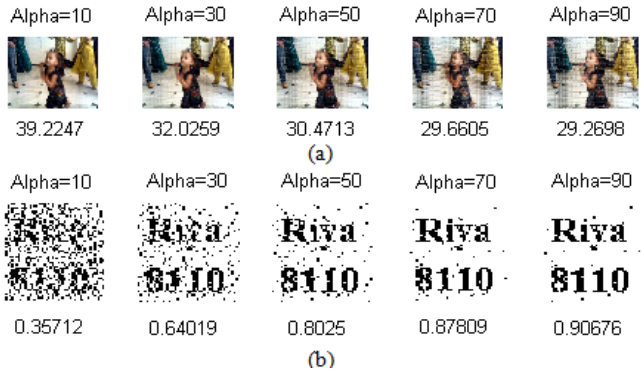
Figure 3. Embedding Process – Results Gain factor-100

Table 1 : Results Gain factor-100 with MSE

Frame No.	PSNR(dB)	MSE	Correlation
1	29.1594	78.912	0.9157
2	29.2581	77.1381	0.9139
3	27.7918	108.1186	0.9124
4	29.7354	69.1104	0.9263
5	29.2402	77.4563	0.9192

Table 2 : Results with different α value

Alpha	PSNR(dB)	MSE	Correlation
1	47.1969	1.2399	0.0883
2	46.8045	1.3572	0.1229
3	46.169	1.571	0.1498
4	44.5424	2.2848	0.1921
5	43.6855	2.7831	0.2117
6	42.8014	3.4115	0.2409
7	42.0538	4.0522	0.2693
8	41.3113	4.8078	0.3063
9	40.5757	5.6952	0.321
10	39.2247	7.7734	0.3571
100	29.1594	78.912	0.9157



1. Perceptibility and Gain Factor:

• Perceptibility decreases with an increase in the gain factor used for watermark embedding.

• Robustness, however, increases with an increase in the gain factor.

2. Quality Metrics:

- Frames appear visually fine if the resultant Peak Signal-to-Noise Ratio (PSNR) is above 28 dB.
- The embedded message is visibly identifiable if the resultant correlation is greater than 0.50.

3. Robustness Against Attacks:

- Not robust against average filtering, median filtering, rotation, and high-pass filtering attacks
- Partially robust against Gaussian low-pass filtering, compression, linear motion of the camera, Gaussian noise, salt & pepper noise, and speckle noise attacks.
- Fully robust against colour reduction and cropping attacks.

7. Conclusion

The study reveals a nuanced relationship between perceptibility and robustness in the context of invisible watermarking, primarily influenced by the gain factor employed during the embedding process. As the gain factor increases, perceptibility diminishes, suggesting a successful integration of the watermark without noticeable alterations to the original frames. Concurrently, robustness against various attacks improves with a higher gain factor, indicating a trade-off between imperceptibility and resilience to manipulation.

The criterion for visual quality, as measured by the Peak Signal-to-Noise Ratio (PSNR), establishes a threshold of 28 dB for frames to appear visibly fine. Moreover, the detectability of the embedded message relies on achieving a resultant correlation greater than 0.50, emphasizing the importance of correlation metrics in watermark identification. While the system exhibits notable robustness against colour reduction and cropping attacks, it falls short against certain filtering and rotation operations. Specifically, it is not robust against average filtering, median filtering, rotation, and high-pass filtering attacks. However, it demonstrates partial resilience against Gaussian low-pass filtering, compression, linear motion of the camera, Gaussian noise, salt & pepper noise, and speckle noise attacks. In conclusion, the invisible watermarking system's performance is intricately linked to the gain factor, with considerations for perceptibility, robustness, and resistance to specific attacks. The study provides valuable insights into the delicate balance required to achieve effective watermarking, taking into account the diverse challenges posed by different forms of image manipulation.

References

[1] Cox, M. L. Miller and J. A. Bloom, “Digital Watermarking,” Morgan Kaufmann Publishers, San Francisco, 2002.

[2] M. Barni and F. Bartolini, “Applications,” in Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications, 1st ed., Boca Raton, New York: CRC Press, 2005, pp. 23–44.

[3] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. on Image Proc.,Vol 6:1673-1687,1997

[4] C. I. Podilchuk and E. J. Delp, "Digital watermarking: algorithms and applications," in *IEEE Signal Processing Magazine*, vol. 18, no. 4, pp. 33-46, July 2001,

[5] Swaminathan, Yinian Mao and Min Wu, "Robust and secure image hashing," in *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 215-230, June 2006,

[6] A. M. Alattar, "Reversible watermark using difference expansion of triplets," *Proceedings 2003 International Conference on Image Processing (Cat. No.03CH37429)*, Barcelona, Spain, 2003, pp. I-501,

[7] SaeidFazli, Masoumeh Moeini "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks",Optik,Volume 127, Issue 2,2016, pp 964-972,

[8] M. Barni, F. Bartolini, A. De Rosa and A. Piva, "Optimum decoding and detection of multiplicative watermarks," in *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1118-1123, April 2003

[9] RohitThanki, Ashish Kothari, DevenTrivedi, "Hybrid and blind watermarking scheme in DCuT – RDWT domain" Journal of Information Security and Applications, Volume 46, Pages 231-249,2019,

[10] RohitThanki and Ashish Kothari, Multi-level security of medical images based on encryption and watermarking for telemedicine applications. Multimedia Tools Appl. 80, 4307–4325,2021

[11] Thanki, Rohit M., and Ashish M. Kothari. "Hybrid domain watermarking technique for copyright protection of images using speech watermarks." Journal of Ambient Intelligence and Humanized Computing 11, no. 5 (2020): 1835-1857.

[12] Raymond B. Wolfgang, Christine I. Podilchuk, "Perceptual watermarks for digital images and video" Proceedings of the IEEE, Volume:87, Number:7, July 1999.

[13] Gerhard C. Langelaar, IwanSetyawan, Reginald L. Lagendijk, "Watermarking of digital image and video data – A state of art review", IEEE signal processing magazine, page: 20-46, September 2000.

[14] Podilchuk, C.I., Delp, E.J., 2001. Digital watermarking: Algorithms and applications. IEEE Signal Process. Mag. 18 (4), 33–46.

[15] R. Chandramouli, N. D. Memon, and M. Rabbani, "Digital watermarking," in Encyclopedia of Imaging Science and Technology. New York: Wiley, 2002.