Publications

Educational Administration: Theory and Practice
2024, 30(6)(s), 110-117
ISSN: 2148-2403
https://kuey.net/
Research Article

Educational Administration Theory and Practice

A Novel Approach To Achieve Dual Security In Images Using Advanced Watermarking Technique

Kiran Pithiya[1*], Kothari Ashish M[2]

[1*]Research Scholar, Department of Electronics and Communication Engineering, Atmiya University, Rajkot, India,
Email:-pithiyakiran8@gmail.com
[2]Professor, Department of Electronics and Communication Engineering, Atmiya University, Rajkot, India,
Email:-ashish.kothari@atmiyauni.ac.in

***Corresponding author:**- Kiran Pithiya
Email:-pithiyakiran8@gmail.com

Citation: Kiran Pithiya, et al. (2024) A Novel Approach To Achieve Dual Security In Images Using Advanced Watermarking Technique *Educational Administration: Theory and Practice*, 30(6)(s) 110-117
Doi: 10.53555/kuey.v30i6(S).5335

ARTICLEINO	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.

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.

II 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) drived and devloped 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.
This reference 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.

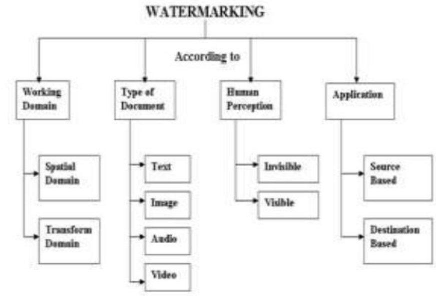


Figure 1 (a) Water Marking Scheme

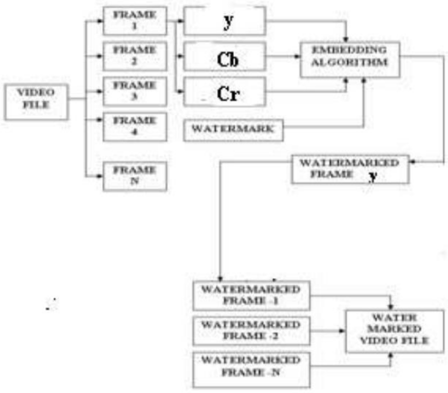


Figure 1(b) General Idea of Digital Watermarking

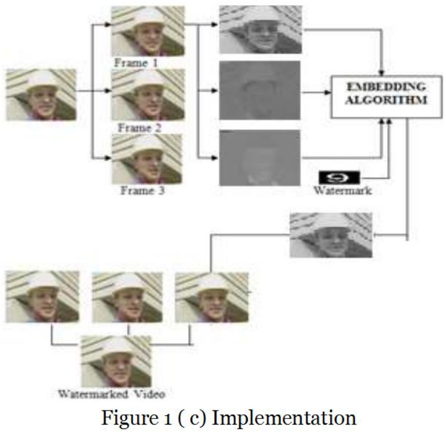


Figure 1 (c) Implementation

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.

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. Here, we'll discuss the importance of both visible and invisible watermarks in achieving dual security:

III 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.

IV 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.

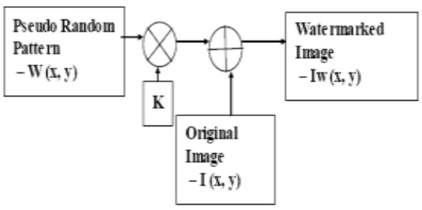


Figure 2 . Two Processes – one for watermark bit 0 and the other for bit 1

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.

V 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.

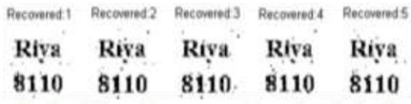


Figure 3. Embedding Process – Results Gain factor-100

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

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

Table 2 : Results with different α value

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.

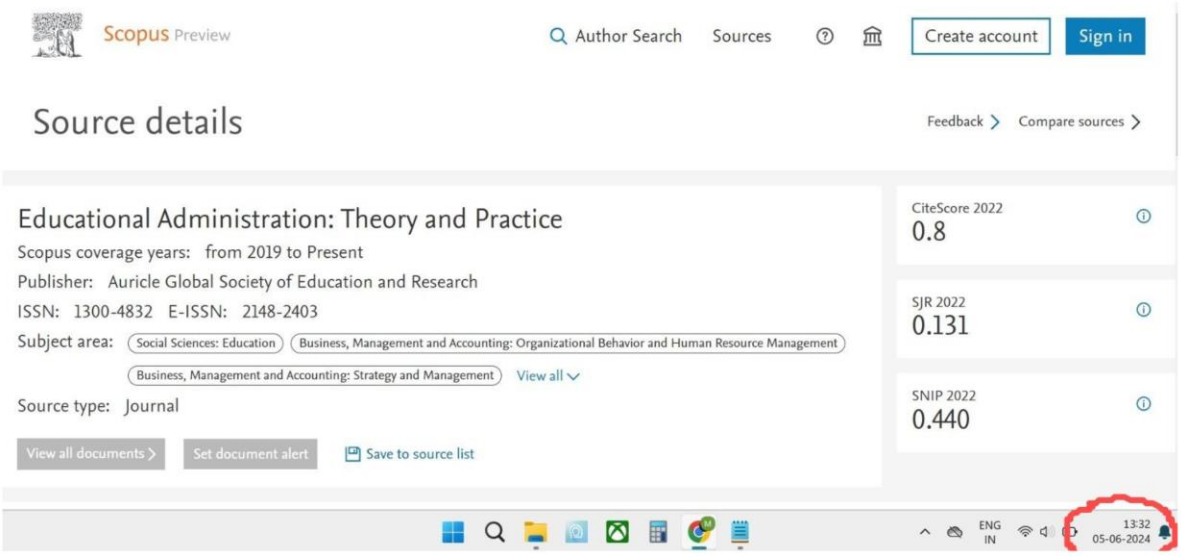
VI CONCLUSION

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.


Scopus Preview
Author Search
Sources
Create account
Sign in
Source details
Feedback
Compare sources
Educational Administration: Theory and Practice
Scopus coverage years: from 2019 to Present
Publisher: Auricle Global Society of Education and Research
ISSN: 1300-4832 E-ISSN: 2148-2403
Subject area: Social Sciences: Education
Business, Management and Accounting: Organizational Behavior and Human Resource Management
Business, Management and Accounting: Strategy and Management
View all
Source type: Journal
View all documents
Set document alert
Save to source list
CiteScore 2022
0.8
SJR 2022
0.131
SNIP 2022
0.440
ENG
IN
13:32
05-06-2024

Educational Administration: Theory and Practice
2024, 30(6s), 346-350
ISSN: 2148-2403
https://kuey.net/
Research Article

Watermark The Region Of Interest In Image - An SVD Based Approach

Kiran Pithiya[1*], Kothari Ashish M[2]

[1*]Research Scholar, Department of Electronics and Communication Engineering, Atmiya University, Rajkot, India, pithiyakiran8@gmail.com
[2]Professor, Department of Electronics and Communication Engineering, Atmiya University, Rajkot, India, ashish.kothari@atmiyauni.ac.in

Citation Kiran Pithiya (2024), Watermark The Region Of Interest In Image - An SVD Based Approach, *Educational Administration: Theory and Practice, 30(6s)*, 346-350, Doi: 10.53555/kuey.v30i6(S).6117

ARTICLE INFO | **ABSTRACT**

This paper introduces a novel method for embedding watermark messages into the crucial part of an image, specifically the region of interest (ROI). The focus is on identifying the human face within an image and embedding the watermark within this detected face. Once the watermark is embedded, the altered face image is reinserted back into the original image. To achieve this, the method employs a face identification algorithm alongside the powerful linear algebra technique known as Singular Value Decomposition (SVD). Additionally, the paper utilizes three widely recognized visual quality metrics to evaluate the method's effectiveness. At the transmitter side, Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are used to assess the perceptual quality of the image after watermark embedding. At the receiver side, correlation is measured to test the robustness of the algorithm.

Keywords: Digital Image Watermarking, Singular Value Decomposition, Region of Interest, Perceptibility, Robustness

INTRODUCTION

Digital watermarking is a process used to embed information into a digital signal, such as an image, audio, or video, in a way that is difficult to remove and does not significantly degrade the signal quality. This embedded information, known as a watermark, can be used for various purposes, including copyright protection, authentication, and content tracking. It is a crucial technology for protecting digital content in an increasingly digital world. By embedding hidden information within media files, it provides a means of asserting ownership, verifying authenticity, and tracking content usage. Advances in watermarking techniques continue to improve the balance between imperceptibility, robustness, security, and capacity, making it an essential tool for digital rights management and content protection.

SINGULAR VALUE DECOMPOSITION

Singular Value Decomposition (SVD) is a fundamental numerical technique rooted in linear algebra, widely used across various fields including image processing. When applied to an image matrix A of size M×N, SVD decomposes it into three matrices: U, S and V:

- **Representation**: The decomposition is represented as $A = USV^T$
- **Unitary Matrices**: U and V are unitary matrices of sizes M×M and N×N respectively.
- **Diagonal Matrix**: S is a diagonal matrix of size M×N where the diagonal entries are the singular values of A.
- **Singular Values**: These values are crucial for watermarking as they are stable and reflect the intrinsic properties of the image.
- **Stability**: Small changes in the original image A do not lead to significant changes in its singular values, making SVD a robust technique for image analysis and processing.
- **Brightness and Geometry**: Singular values correspond to the brightness levels of the image, while singular vectors (columns of U and V) represent geometric features.
- **Significance of Singular Values**: The first singular value dominates, with subsequent values being smaller. Omitting these smaller values typically results in negligible perceptual changes in the reconstructed image.

SVD's ability to decompose an image matrix into these components allows for efficient representation and manipulation in various applications, including image compression, noise reduction, and watermark embedding. Its robustness and stability make it particularly suitable for tasks where preserving image quality and content integrity are paramount.
One example of the SVD process is explained in the table 1.

Original Matrix		
1	2	3
4	5	6
7	8	9
10	11	12

U Matrix			
0.140877	-0.82471	-0.54556	0.048576
0.343946	-0.42626	0.691212	-0.47141
0.547016	-0.02781	0.254268	0.797087
0.750086	0.370637	-0.39992	-0.37426

V Matrix		
0.504533	0.760776	0.408248
0.574516	0.057141	-0.8165
0.644498	-0.64649	0.408248

S Matrix		
25.46241	0	0
0	1.290662	0
0	0	1.46E-15
0	0	0

Table 1: Example of SVD

VISUAL QUALITY PARAMETERS

We primarily utilized the following visual quality metrics to compare the degradation observed after adding the watermark to the image:

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} \{(f(x,y) - f'(x,y))^2\} \quad (1)$$

$$PSNR = 10 \times \log \frac{255^2}{MSE} \quad (2)$$

Here
- MSE – Mean Square Error
- PSNR – Peak Signal to Noise Ratio
- f(x,y) – Original Frame of the video
- f'(x,y) – Watermarked Frame of the Video.

The term "Peak Signal-to-Noise Ratio" (PSNR) is commonly used to quantify the similarity between two signals: one being the original and the other an altered version of the same signal. PSNR is defined using the Mean Square Error (MSE), which provides insight into the differences between the original and altered signals. PSNR is expressed in a logarithmic scale, offering a standardized measure of signal fidelity. In contrast, MSE is measured in a straightforward numerical scale. After extracting the watermark at the receiver's end, we assess its robustness by measuring the correlation between the recovered watermark and the original watermark. This correlation test helps evaluate how well the watermark survived various signal distortions or attacks, providing a measure of the watermarking system's resilience to tampering and ensuring reliable detection of the embedded information.

PROPOSED METHOD

The proposed algorithm is a novel approach as compare to the approaches given till time as in this algorithm the watermarking is done on the region of interest (in this case - Face) of the image only rather than watermarking the entire image.

Embedding Algorithm and Results

Here is a step-by-step explanation of the process used to embed a message behind the face part of an image:
1. **Face Detection**: Faces are identified and located within the image using algorithms such as Viola-Jones or deep learning-based detectors.
2. **Colorspace Conversion**: The RGB frame of each detected face is converted into the YCbCr colorspace.
3. **Selection of Y Frame**: The luminance component (Y frame) of the YCbCr colorspace is chosen for embedding the grayscale message.
4. **Singular Value Decomposition (SVD)**: SVD is applied to the selected Y frame to decompose it into three matrices: U, S, and V.
5. **Watermark Rescaling**: The grayscale watermark (W) intended for embedding is resized to match the dimensions of the singular component matrix S obtained from the SVD.
6. **Modification of Singular Component**: The singular component S is modified as S = S + K * W, where K is a gain factor that determines the strength of the watermark embedding.
7. **SVD Reapplication**: SVD is reapplied to the modified singular component to obtain new matrices U, S', and V.
8. **Modification of Selected Sub-band**: The modified singular component S' is used to reconstruct the altered luminance component: New_Value = U * S' * V^T.
9. **Inverse Colorspace Conversion**: The modified YCbCr frame is converted back to RGB colorspace.

10. **Reinsertion of Altered Face Image**: The watermarked face image, now containing the embedded watermark, is reinserted back into its original position within the image.
11. **PSNR and MSE Calculation**: The Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) are computed to assess the perceptual quality and fidelity of the watermarked image compared to the original. These metrics help evaluate how well the embedded watermark has been integrated into the image without introducing noticeable degradation.

This method ensures that the message is securely embedded behind the face part of the image while preserving the overall quality and integrity of the image content, specifically focusing on the detected faces.

Figure 1: Original Image

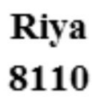


Figure 2: Original Message

Figure 3 : Extracted Faces

Figure 4 : Watermarked Image
@ Gain factor = 10

Gain Factor	PSNR	MSE
10	53.91	0.26
20	48.23	0.97
50	42.99	3.25

Table 2: Perceptibility at Various Gain Factor

Extracting Algorithm and Results

Here's a step-by-step explanation of how the watermark is extracted from the face part of an image:

1. **Face Detection**: Faces are identified and located within the watermarked image using algorithms designed for face detection.
2. **Colorspace Conversion**: The RGB frame containing the detected face is converted into the YCbCr colorspace.
3. **Selection of Y Frame**: The luminance component (Y frame) of the YCbCr colorspace, corresponding to the detected face, is chosen for extracting the watermark.
4. **Singular Value Decomposition (SVD)**: SVD is applied to the selected Y frame to decompose it into three matrices: U, S, and V.
5. **Resizing Singular Component**: The singular component (S) obtained from SVD is resized to match the size of the watermark message, resulting in $D = U * S * V^T$.
6. **Watermark Extraction**: The watermark is extracted by computing (D - S) / K, where K is a scaling factor used during the watermark embedding process.
7. **Correlation Calculation**: The correlation coefficient between the original watermark and the recovered watermark is computed. This correlation value serves as a measure of the algorithm's robustness, indicating how well the embedded watermark was preserved and recovered from the watermarked image.

This process ensures that the watermark embedded in the face part of the image can be accurately extracted, demonstrating the effectiveness and reliability of the watermarking algorithm in maintaining the integrity and security of the embedded information.

Gain Factor = 10

Gain Factor = 20

Gain Factor = 50

Figure 5: Extracted Watermarks at Various Gain Factors

Gain Factor	Correlation
10	0.9913
20	0.9902
50	0.9815

Table 3: Robustness at Various Gain Factor

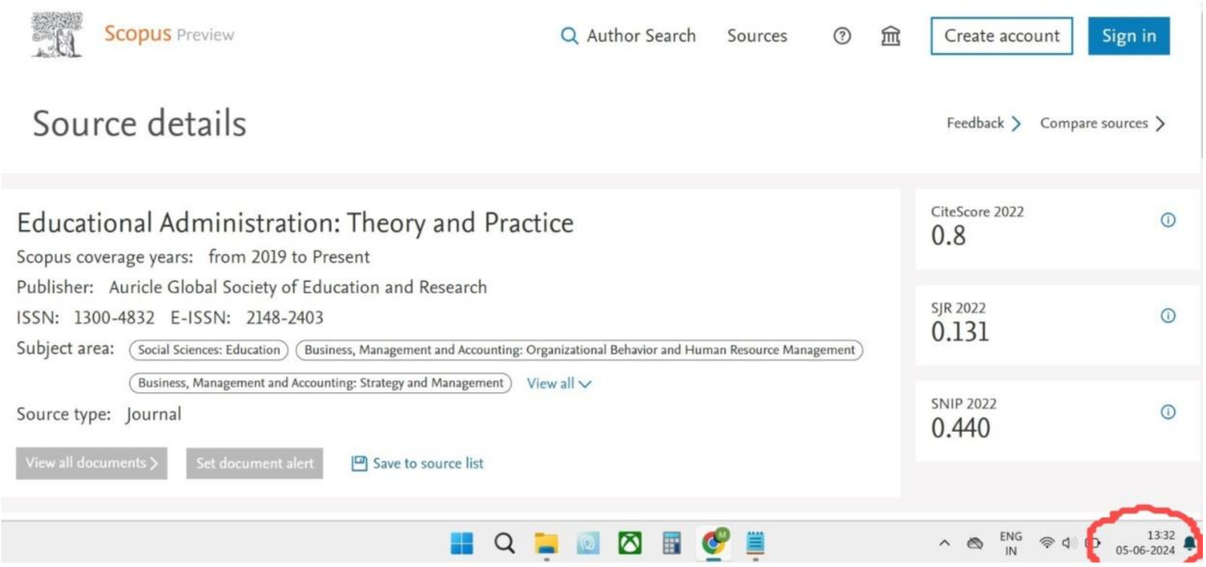
OBSERVATIOS / CONCLUSION

- Perceptibility decreases with the increase in gain factor.
- Robustness decreases with the increase in gain factor.
- The frames looks visibly fine if the resultant PSNR is above 28 dB. The message seems visibly identifiable if the resultant correlation is greater than 0.50.
- SVD gives better results as compare to spatial domain and transform domain techniques so far as Perceptibility and Robustness is concerned.

REFERENCES

1. **Cox, M. L. Miller and J. A. Bloom, “Digital Watermarking,” Morgan Kaufmann Publishers, San Francisco, 2002.**
   This foundational book provides a comprehensive overview of digital watermarking techniques, applications, and technologies.
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.**
   Discusses practical applications of watermarking systems in ensuring security for digital assets.
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.**
   Introduces secure spread spectrum watermarking techniques for multimedia content, focusing on robustness and security.
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.**
   Provides an overview of algorithms and applications of digital watermarking, highlighting advancements and challenges.
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.**
   Discusses robust and secure image hashing techniques, which are related to watermarking for content authentication.
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.**
   Introduces a reversible watermarking technique based on difference expansion, suitable for multimedia applications.
7. **Saeid Fazli, 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.**
   Proposes a robust image watermarking method utilizing wavelet, discrete cosine, and singular value decompositions to mitigate geometric attacks.
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.**
   Focuses on optimum decoding and detection methods for multiplicative watermarks, enhancing watermark detection reliability.
9. **Rohit Thanki, Ashish Kothari, Deven Trivedi, “Hybrid and blind watermarking scheme in DCuT – RDWT domain” Journal of Information Security and Applications, Volume 46, Pages 231-249, 2019.**
   Discusses a hybrid and blind watermarking scheme using dual-tree complex wavelet transform and redundant discrete wavelet transform.
10. **Rohit Thanki and Ashish Kothari, "Multi-level security of medical images based on encryption and watermarking for telemedicine applications," Multimedia Tools Appl. 80, 4307–4325, 2021.**
    Explores multi-level security approaches for medical images using encryption and watermarking techniques tailored for telemedicine applications.

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.** Presents a hybrid domain watermarking technique employing speech watermarks for copyright protection of images.
12. **Raymond B. Wolfgang, Christine I. Podilchuk, "Perceptual watermarks for digital images and video" Proceedings of the IEEE, Volume:87, Number:7, July 1999.** Discusses perceptual watermarks designed for digital images and videos, emphasizing imperceptibility and robustness.
13. **Gerhard C. Langelaar, Iwan Setyawan, Reginald L. Lagendijk, "Watermarking of digital image and video data – A state of art review", IEEE signal processing magazine, pages 20-46, September 2000.**
    Provides a comprehensive review of watermarking techniques for digital image and video data, covering state-of-the-art advancements.
14. **Podilchuk, C.I., Delp, E.J., 2001. Digital watermarking: Algorithms and applications. IEEE Signal Process. Mag. 18 (4), 33–46.**
    Further discusses algorithms and applications of digital watermarking, focusing on practical implementations and challenges.
15. **R. Chandramouli, N. D. Memon, and M. Rabbani, "Digital watermarking," in Encyclopedia of Imaging Science and Technology. New York: Wiley, 2002.**
    Provides an encyclopedia entry covering various aspects of digital watermarking, including techniques, applications, and challenges.


Scopus Preview
Author Search
Sources
Create account
Sign in
Source details
Feedback
Compare sources
Educational Administration: Theory and Practice
Scopus coverage years: from 2019 to Present
Publisher: Auricle Global Society of Education and Research
ISSN: 1300-4832 E-ISSN: 2148-2403
Subject area: Social Sciences: Education
Business, Management and Accounting: Organizational Behavior and Human Resource Management
Business, Management and Accounting: Strategy and Management
View all
Source type: Journal
View all documents
Set document alert
Save to source list
CiteScore 2022
0.8
SJR 2022
0.131
SNIP 2022
0.440
ENG
IN
13:32
05-06-2024