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

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:

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

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

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.

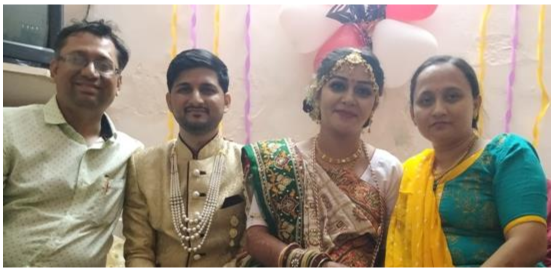


Figure 1: Original Image

Figure 2: Original Message

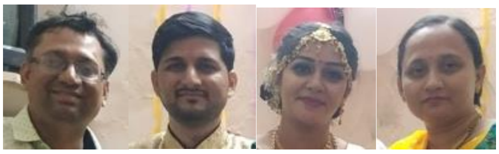


Figure 3 : Extracted Faces

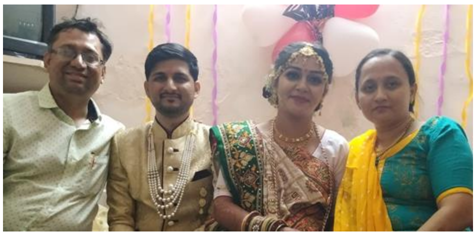


Figure 4 : Watermarked Image
@ Gain factor = 10

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

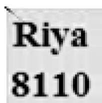
Here's a step-by-step explanation of how the watermark is extracted from the face part of an image:

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.