Lecture Notes in Networks and Systems 1439

Aboul Ella Hassanien
Sameer Anand
Ajay Jaiswal
Prabhat Kumar *Editors*

Innovative Computing and Communications

Proceedings of ICICC 2025, Volume 10

Springer

Lecture Notes in Networks and Systems

Volume 1439

The series "Lecture Notes in Networks and Systems" publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, EI Compendex, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

For proposals from Asia please contact Aninda Bose (aninda.bose@springer.com).

Aboul Ella Hassanien · Sameer Anand ·
Ajay Jaiswal · Prabhat Kumar
Editors

Innovative Computing and Communications

Proceedings of ICICC 2025, Volume 10

Springer

Editors
Aboul Ella Hassanien
Faculty of Computer and Information
Cairo University
Giza, Egypt

Ajay Jaiswal
Department of Distance and Continuing
Education, School of Open Learning
Campus of Open Learning
University of Delhi
New Delhi, Delhi, India

Sameer Anand
Department of Operational Research
Faculty of Mathematical Sciences
University of Delhi
New Delhi, Delhi, India

Prabhat Kumar
Department of Computer Science
and Engineering
National Institute of Technology Patna
Patna, Bihar, India

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-981-96-7136-6 ISBN 978-981-96-7137-3 (eBook)
https://doi.org/10.1007/978-981-96-7137-3

ICICC-2025 Steering Committee Members

Patrons

Dr. Poonam Verma, Principal, SSCBS, University of Delhi
Prof. Dr. Pradip Kumar Jain, Director, National Institute of Technology Patna, India

General Chairs

Prof. Dr. Bal Virdee, London Metropolitan University, London, UK
Prof. (Dr.) Prabhat Kumar, National Institute of Technology Patna, India

Honorary Chairs

Prof. Dr. Janusz Kacprzyk, FIEEE, Polish Academy of Sciences, Poland
Prof. Dr. Vaclav Snasel, Rector, VSB-Technical University of Ostrava, Czech Republic

Conference Chairs

Prof. Punam Bedi, Department of Computer Science, University of Delhi
Prof. Dr. R. K. Agrawal, Jawaharlal Nehru University, Delhi

Technical Program Chairs

Prof. Dr. A. K. Singh, National Institute of Technology, Kurukshetra
Dr. Kumar Bijoy, Associate Professor, Shaheed Sukhdev College of Business Studies, Delhi University

Editorial Chairs

Prof. Dr. Abhishek Swaroop, Bhagwan Parshuram Institute of Technology, Delhi
Prof. Aboul Ella Hassanien, Cairo University, Egypt

Conveners

Prof. Ajay Jaiswal, Department of Distance and Continuing Education, School of Open Learning, Campus of Open Learning, University of Delhi, India
Dr. Sameer Anand, Department of Operational Research, University of Delhi, India

Publicity Chairs

Dr. Jafar A. Alzubi, Al-Balqa Applied University, Salt, Jordan
Dr. Hamid Reza Boveiri, Sama College, IAU, Shoushtar Branch, Shoushtar, Iran

Co-Conveners

Dr. Moolchand Sharma, Maharaja Agrasen Institute of Technology, India
Dr. Jameel Ahmed, Maulana Azad National Urdu University (MANUU), Hyderabad, India
Dr. Amrina Kausar, Associate Professor, Shaheed Sukhdev College of Business Studies, Delhi University

Organizing Chairs

Dr. Rishi Rajan Sahay, Associate Professor, Vice Principal, Shaheed Sukhdev College of Business Studies, Delhi University
Dr. Gulshan Shrivastava, Associate Professor, Bennett University, Greater Noida, India

Preface

We hereby are delighted to announce that Shaheed Sukhdev College of Business Studies, New Delhi, in association with National Institute of Technology Patna, and University of Valladolid Spain has hosted the eagerly awaited and much coveted International Conference on Innovative Computing and Communication (ICICC-2025) in hybrid mode. The eight version of the conference was able to attract a diverse range of engineering practitioners, academicians, scholars, and industry delegates, with the reception of abstracts including more than 5000 authors from different parts of the world. The committee of professionals dedicated toward the conference is striving to achieve a high-quality technical program with tracks on innovative computing, innovative communication network and security, and Internet of Things. All the tracks chosen in the conference are interrelated and are very famous among the present-day research community. Therefore, a lot of research is happening in the above-mentioned tracks and their related sub-areas. As the name of the conference starts with the word "innovation," it has targeted out-of-box ideas, methodologies, applications, expositions, surveys, and presentations helping to upgrade the current status of research. More than 1800 full-length papers have been received, among which the contributions are focused on theoretical, computer simulation-based research, and laboratory-scale experiments. Among these manuscripts, 20% of the papers have been included in the Springer proceedings after a thorough two-stage review and editing process. All the manuscripts submitted to the ICICC-2025 were peer-reviewed by at least two independent reviewers, who were provided with a detailed review proforma. The comments from the reviewers were communicated to the authors, who incorporated the suggestions in their revised manuscripts. The recommendations from two reviewers were taken into consideration while selecting a manuscript for inclusion in the proceedings. The exhaustiveness of the review process is evident, given the large number of articles received addressing a wide range of research areas. The stringent review process ensured that each published manuscript met the rigorous academic and scientific standards. It is an exalting experience to finally see these elite contributions materialize into ten book volumes as ICICC-2025 proceedings by Springer entitled "International Conference on Innovative Computing and Communications." The articles are organized into three volumes

in some broad categories covering subject matters on machine learning, data mining, big data, networks, soft computing, and cloud computing, although given the diverse areas of research reported, it might not have been always possible.

ICICC-2025 invited six keynote speakers, who are eminent researchers in the field of computer science and engineering, from different parts of the world. In addition to the plenary sessions on each day of the conference, thirty-two concurrent technical sessions are held on both days to assure the oral presentation of around 400 accepted papers. Keynote speakers and session chair(s) for each of the concurrent sessions have been leading researchers from the thematic area of the session. A technical exhibition is held during all the 2 days of the conference, which has put on display the latest technologies, expositions, ideas, and presentations. The research part of the conference was organized in a total of 41 special sessions. These special sessions and international workshops provided the opportunity for researchers conducting research in specific areas to present their results in a more focused environment.

An international conference of such magnitude and release of the ICICC-2025 proceedings by Springer have been the remarkable outcome of the untiring efforts of the entire organizing team. The success of an event undoubtedly involves the painstaking efforts of several contributors at different stages, dictated by their devotion and sincerity. Fortunately, since the beginning of its journey, ICICC-2025 has received support and contributions from every corner. We thank them all who have wished the best for ICICC-2025 and contributed by any means toward its success. The edited proceedings volumes by Springer would not have been possible without the perseverance of all the steering, advisory, and technical program committee members.

All the contributing authors owe thanks from the organizers of ICICC-2025 for their interest and exceptional articles. We would also like to thank the authors of the papers for adhering to the time schedule and for incorporating the review comments. We wish to extend my heartfelt acknowledgment to the authors, peer-reviewers, committee members, and production staff whose diligent work put shape to the ICICC-2025 proceedings. We especially want to thank our dedicated team of peer-reviewers who volunteered for the arduous and tedious step of quality checking and critique on the submitted manuscripts. We wish to thank my faculty colleagues Dr. Moolchand Sharma, Dr. Jameel Ahmed, and Dr. Simar Preet Singh for extending their enormous assistance during the conference. The time spent by them and the midnight oil burnt is greatly appreciated, for which we will ever remain indebted. The management, faculties, administrative, and support staff of the college have always been extending their services whenever needed, for which we remain thankful to them.

Lastly, we would like to thank Springer for accepting our proposal for publishing the ICICC-2025 conference proceedings. Help received from Mr. Aninda Bose, the acquisition senior editor, in the process has been very useful.

Giza, Egypt — Aboul Ella Hassanien
New Delhi, India — Sameer Anand
New Delhi, India — Ajay Jaiswal
Patna, India — Prabhat Kumar
Conveners, ICICC-2025

Contents

About the Editors

Dr. (Prof.) Aboul Ella Hassanien is the Founder and Head of the Egyptian Scientific Research Group (SRGE). He has authored over 1000 research papers in esteemed international journals and more than 50 books spanning data mining, medical imaging, intelligent systems, social networks, and smart environments. He has received numerous accolades, including the Best Researcher of the Youth Award in Astronomy and Geophysics from the National Research Institute (Egypt, 1990), the Scientific Excellence Award in Humanities from the University of Kuwait (2004), and the Superiority of Scientific-University Award from Cairo University (2013). He was also recognized as the best researcher at Cairo University in 2013 and received the ISESCO Prize for Technology in 2014.

Prof. Sameer Anand is a Professor in the Department of Operational Research, Faculty of Mathematical Sciences, University of Delhi. He holds M.Sc., M.Phil., and Ph.D. degrees in Software Reliability, all from the University of Delhi. He received the "Best Teacher Award" (2012) from the Directorate of Higher Education, Government of NCT, Delhi. He serves as an Associate Editor for the *International Journal of System Assurance Engineering and Management*. His research focuses on software reliability, mathematical modeling, optimization, supply chain management, and machine learning. He has published over 45 research papers in reputed journals, including *IEEE Transactions on Reliability, Expert Systems*, and the *International Journal of Production Research* (Taylor & Francis). He has also edited seven books comprising 17 volumes. Before joining the university department, he held roles such as Professor, Vice Principal, and Officiating Principal at Shaheed Sukhdev College of Business Studies, DU.

Prof. Ajay Jaiswal has an academic background from prestigious institutions like IIT Roorkee and JNU. With over 25 years of experience in academics, research, and administration, he currently serves as the Principal of the School of Open Learning, University of Delhi. Additionally, he holds the position of OSD at the Institute of Cyber Security Law, University of Delhi. A prolific author and researcher, he has contributed to numerous research articles and books and has been actively involved

in editorial and organizing committees for journals and international conferences. His research interests include pattern recognition, image processing, and machine learning. He was honored as the "Best Teacher" by the Government of NCT Delhi for 2013–14.

Dr. (Prof.) Prabhat Kumar is a Professor in Computer Science and Engineering at NIT Patna, India. He holds multiple administrative roles, including Chief Proctor and Head of the Centre for Computing and Information Services. Previously, he served as Head of the CSE Department and State Student Coordinator for Bihar in CSI. A senior member of IEEE and a professional member of ACM, he is part of National Working Group 13 (NWG-13) for ITU-T Study Group 13, focusing on future networks and cloud computing. He has over 150 publications in reputed journals and conferences, three authored books, two completed research projects, and four granted Indian patents. He has supervised 13 Ph.D. and 28 M.Tech. scholars, chaired international conferences, and reviewed SCI/Scopus-indexed journals. His research interests include wireless sensor networks, IoT, data analytics, software engineering, and e-governance.

Chapter 1
Resilient Video Watermarking Algorithm Employing Cryptography and Moving Frames

Shalaka Tyagi, Priya Sharma, Santosh Kumar, Nitesh Singh Bhati, and Lalitesh Chaudhary

Abstract These days, fast Internet connections allow audio and video files to be sent swiftly. Accurate copies of the underlying audio and video content can now be produced more easily because of the advancement of these techniques. The creation of such exact clones exposes the malicious consumer's false claim to ownership of digital content. The recommended method to fight against these types of misleading claims is to give some videos an authenticity label. During placement, the logo is first jumbled using a method authorized by an encryption password. The given key can be used to understand the logo when necessary. A tiny mark is applied to the standard image using the SVD and DWT techniques. According to the suggested strategy's decisions, the structure is safe and impervious to a variety of intentional and unintentional hazards. It is displayed since the recommended method is more effective at stopping malicious people from employing computers to make misleading claims.

Keywords Motion frames · Singular value · Video watermarking · Wavelet transform

Priya Sharma and Lalitesh Chaudhary: These authors contributed equally to this work.

S. Tyagi
Sharda School of Engineering and Technology, Sharda University, Greater Noida, Uttar Pradesh, India

P. Sharma · L. Chaudhary
School of Computer Science Engineering and Technology, Bannett University, Greater Noida, Uttar Pradesh, India

S. Kumar (✉)
School of Computer Applications and Technology, Galgotias University, Greater Noida, Uttar Pradesh, India
e-mail: sant7783@hotmail.com

N. Singh Bhati
Department of Computer Science and Engineering, Gautam Buddha University, Yamuna Expressway, Greater Noida, Uttar Pradesh, India

A. E. Hassanien et al. (eds.), *Innovative Computing and Communications*, Lecture Notes in Networks and Systems 1439, https://doi.org/10.1007/978-981-96-7137-3_1

1.1 Overview

The spread of audiovisual content across different operating systems is encouraged by the expansion of Internet access. The likelihood that audio and video recordings will be safeguarded is reduced by the high-frequency agreement. Ownership, physical confirmation, safeguarding intellectual property, and other issues are among the challenges brought about by the emergence of digital media. In terms of telecommunication copyright protections, technological duplicity is one of the primary problems. The appropriate measures must be implemented to stop such unauthorized individuals from reading the material. Safeguarding information during distribution is made possible via security. No matter the cryptographic key, the malicious party is unable to access or change the computer's contents. In order to generate the original data, the approach uses encryption programs to encrypt information at the consumer's consented endpoint and decrypt it at the destination's endpoint. Establishing a trustworthy and secure system is necessary to stop illegal amusement reproduction and misleading claims of media content on the Internet. Though they still persist, the introduction of fingerprint technologies provides a practical solution to these problems.

Digital watermarks are practical way to add more information about both at the same time when viewing media files. It is possible to electronically apply watermarks to photography and multi-media files. Watermarks are utilized as proof of trademark security anytime they are applied on the original creator's videotape before being retrieved via a method that eliminates a similar logo. Semiconductor methods for watermarking should maintain an appropriate, balanced trade-off between perceptibility, robustness, and cargo. The waterboarding technique limits authorized persons' access to the extraction procedure when copyright protection must be proven. To stop hackers from deleting the protected data, it is best to use a sturdy program that is engraved. We can consider any dark-level graphic, name, brand, time stamps, etc., while deciding on the type of watermarking. These types of watermarked locations are commonly used in several watermarked deployment tactics. Activities, directions, ads, and instructional recordings are just a few of the many types of video material that are constantly flooding the market. Video objects can be divided into two categories: actual origin audiovisual and compression audiovisual [1]. A mix of geographic domain and frequency approaches can be used to watermark the original clip. When implementing the same, a fair trade-off should be established with respect to watermarked attributes. By making a threat, any malevolent person could try to change the material in the video. Incidents fall into four types, such as mathematical threats, activity, and pruning [2]. An additional class of dangers to the visual material are picture enhancement methods like panel recovery, noise reduction, histogram equalization, statistically production, enhanced contrast, and many more. Both planned and inadvertent attacks on media establishments are depicted in the video. According to [3], any malicious user can insert video frames or altered video content from the original source. The usual term for such attacks is unintentional

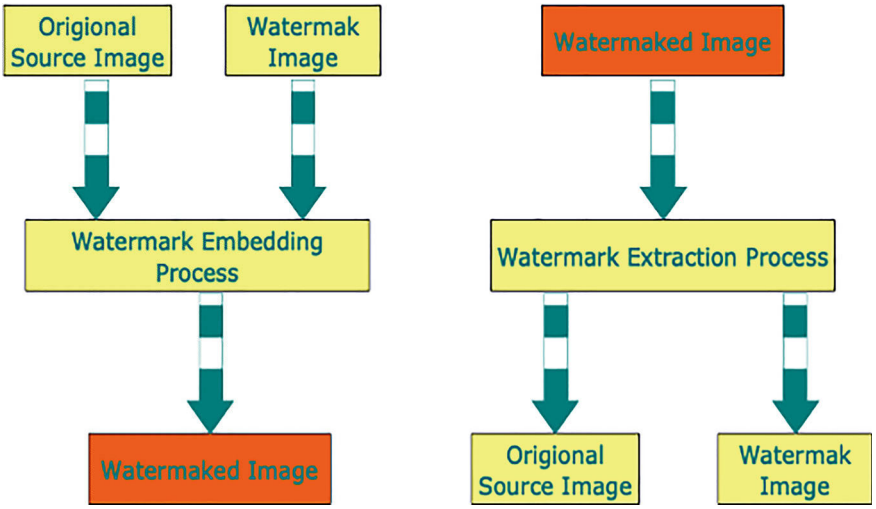

Fig. 1.1 Procedure for electronic engraving

assault. There are deliberate attacks on substitutes of frames. As long as the watermarking system is in use, awareness should continue to be higher than a particular threshold. A distinct feature of the file as the host is maintaining its load capability, which shows how much data needs to be added (Fig. 1.1).

1.2 Context

A signature can be added to a footage using this simple movement sequence. When translating the rapid picture onto a 1-level MR SVD breakdown, the creator first converts the image from RGB to YCbCr color space. Because SVD is applied on every individual estimate, the approach is resilient. The logo is removed from the movie material with a satisfactory perceptibility, and the technique's resilience to various attacks is evaluated [4]. The various applications of watermarking as well as its visual elements. The researchers present the execution techniques, which are separated into two distinct groups: spatial realm and domain of frequencies. A strategy to use a barrel-based deformation algorithm to eliminate the logo from distorted video. The signature is calculated employing association and the mean square error in order to assess the accuracy of the stamp message following the application of the assaults [2]. Applying a watermark using a scrambled watermark over an animated clip. The creator uses unencoded footage to verify the method's reliability. Broadly, the multiple-stage approach is used to jumble the watermark. The privacy feature of the technique is improved by watermark obscuration. The author decides to perform the watermarking procedure on the U element of the YUV formulation. An approach

to microchip anchoring offers methods for decomposing individual values and a separate wavelet transformation. The appearance of the recovered watermark is worse than that of the one that was recovered using the brightness canal, according to SSIM. Following insertion, the suggested method provides an acceptable standard for the audio item [5]. For the purpose of avoiding accidentally embedding the logo in each footage structure, we only do it in images that have a lot of kinetic activity. This method works well because the human visual system is unable to detect tiny details in areas that are moving quickly [6]. The primary objectives of the approach are shot separation and blocking classification. It is an insignificant graphic that is proportional to the dimension of the host file. The chosen frames are then integrated with it [7].

1.3 Approach

1.3.1 Transformation of Continuous Wavelets

Distinctive The kind of mathematical instrument used to carry out the alteration is called waveform shift. A organized set of individual wavelet scales with defined parameters is used. When necessary, the arrangement of coordinates is altered using an algebraic technique called a wavelet. A wavelet transformation converter divides the original signal into a group of wavelets, as opposed to a continuous wavelet change. A scalability equation that describes the scale characteristics of an item can be used to construct the waveform. Wavelet's categorical foundation causes the coefficients there-of to rapidly decrease. There is more information about the thing, like an image, corresponding to the level with higher resolution. With the wavelet, the natural multi-resolution image has all of the image's important edges. The creation along with processing of DWT is particularly appropriate for digitized machines [5]. Wavelet structures having various magnitudes and locations are added and combined to create a picture that has been subjected to the DWT algorithm. In DWT, the pass through and low passage factors reflect the graphic. Here, the graphic is subjected to the high and low filters. After passing via the DWT, the photograph is split into multiple bands of frequencies using the statistical lens. The graphic was divided into 4 subbands using the statistical lenses LL, LH, HL, and HH. It represents the smaller-scale parameters and is occasionally referred to as the initial level of decomposition. Each of the stages of fragmentation is determined by the requirements for implementing the program. The majority of watermarking techniques divide the data into three distinct categories. The term "numerous granularity" describes the idea that electromagnetic impulses are going to be separated between greater accuracy estimates and more minute information. A rougher and tighter estimate is used to represent more precise details regarding the subdomains. The excellent spatiofrequency confinement distinctive of the discrete wavelet transformed method is one of its main advantages [8]. Due to its concealment, DWT is a popular watermarking technology for copyright protective characteristics [9] (Fig. 1.2).

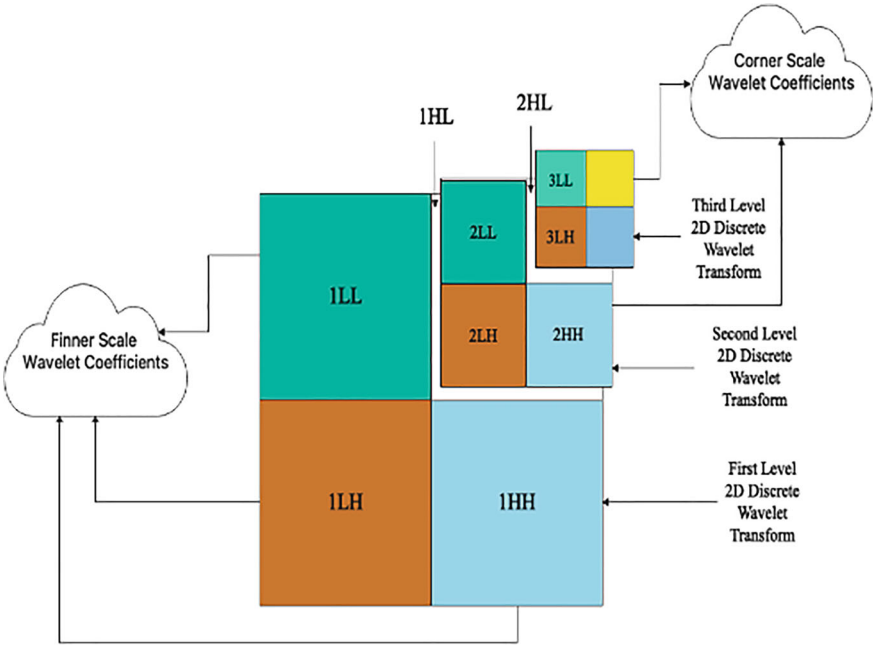

Fig. 1.2 Discrete wavelet transformation levels

1.3.2 The Breakdown of Single Values

In linear equations, a technique for factoring an actual or complicated matrices is called lattice decomposition [10]. Using the extended polar decomposition of a square matrices, the SVD tool generates an m x n matrices. In the SVD, any m x n actual or complexes matrices M will be factorized into UV*, wherein U represents the realistic or complexity unified matrices of dimension m × m. The lateral elements in that rectangle matrices are non-negative, and the configuration is m × n. V is an unilateral matrix, real or intricate, of dimension n × n. The unique denotes the numerical contents of matrices M's orthogonal components.

1.3.3 Watermark Encryption Process

Watermark encryption is employed to protect video within elements because of its rationale. Watermark removal will involve decoding, while watermark implantation will involve encrypting. An enigma key is made for this. The benefit of encrypting is that an unauthorized user cannot rationally decrypt a compressed image. Once the watermark has been deciphered with the hidden key, it is going to be available. It is

Fig. 1.3 Initial insignia

Fig. 1.4 Scramble watermark

shown that the appropriate approach suggested by the author [2] is a reliable way to encode the watermark. The key that will be used to scramble the watermark is first chosen, and it is as outlined below: K = 16, 1, 14, 3, 12, 5, 10, 7, 8, 9, 6, 11, 4, 13, 2, 15. The key that is going to be utilized to scramble the watermark is the arrangement of both even and odd integers. The watermark and the video object will have the same dimensions. The watermark is split up and then rearranged based on the value K that was selected. This phase initiates the encryption of the watermark. Figures 1.3 and 1.4 display a portion of the jumbled watermark and the original watermark, respectively.

To obtain the movement images of the initial raw footage item, the watermark must first be scrambled. The watermarking technique centered around motionless images is quite simple to attack since it relies upon a static portion of the recorded content.

1.3.4 Suggested Watermarking Method

1.3.4.1 Incorporating a Logo

The encrypted portion of the watermark is inserted within the context as a component of the procedure for establishing the scrambled watermark. No grounding

procedure may be carried out if an enclosure which is not a mobility framework is chosen. Movement images alone are used all over the encoding procedure. Restart the encrypted watermark sequence from the beginning if greater numbers of frames are recovered rather than the encrypted parts of the watermark. Next, disentangle an evolving segment's illumination components. The encoding and following independent wavelet translation up to 2-level yielded four subbands: LL, LH, HL, and HH. The watermark is positioned with the HH band. The SVD method applied to this band results in a three-component matrix that is used as the basis for inserting the watermark using a diagonal matrix. In order to watermark the image, a diagonal matrix is employed together with the SVD approach. Implementing watermark embedding requires the following formula.

$$\text{SVDWD} = \text{SVDY} + \alpha\text{SVDw} \tag{1.1}$$

SVDY is the diagonally matrices of the Y element following the application of the SVD procedure. The current value of SVDw, which stands for the diagonal combination of the watermark's panicking, is 0.01. SVDWD is the term for the watermarked design, also known as the diagonally matrices, resulting during the watermarking procedure. In order to create the watermarked movie, the watermark is applied to every screen of the finished product.

1.3.4.2 Elimination of Watermarks

Since we are removing a watermark that has been inserted within an animation frames, we must use the elimination procedure. Check to check if the adjacent RGB frame in the watermarked video is an animated image. It must have a watermark if it is a progression frames graphic. Divide an RGB frame into its Y, Cb, and Cr elements using this method. After that, choose the HH band and apply the level 2 DWT. The diagonal matrix with singular values can be found by using the SVD method. The calculation that follows is used to produce the watermark's unique values.

$$S'_w = \frac{S_o - S_w}{\alpha} \tag{1.2}$$

In the current situation, Sw and So are the sole parameters of the watermarked and real-source footage screen that was recovered. Once you have all the watermarks, follow these steps to get the final one. UW and VW, the diagonal matrices of the watermark, can be used to create a projected watermark. These parameters are known as the initial watermark parameters (Figs. 1.5, 1.6, and 1.7).

$$\text{Watermark} = U_W \times S'_W \times V_W \tag{1.3}$$

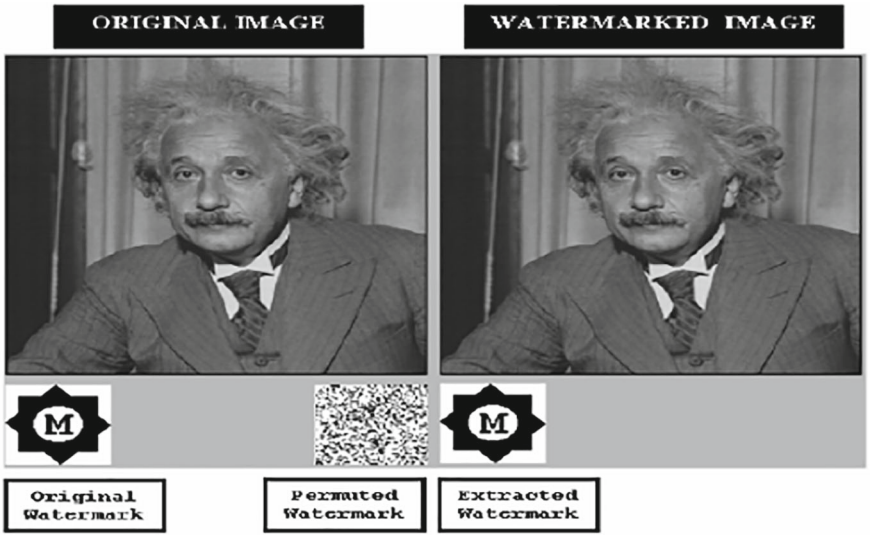

Fig. 1.5 Original and watermarked images

Fig. 1.6 Original and watermarked video frame

1.4 Result and Analysis

Two important aspects need to be examined when the watermark has been retrieved: approach stability and perceptibility. A number of tactics are used to assess the results while watermarking a movie using a removal method. PSNR is one statistic used to gauge perceptibility. Decibels (dBs) are used to determine PSNR. To assess the suggested dependability of the watermarked technology, we look at the aspects of the video. An attempt is made to erase the digital watermark from the watermarked video by continually attacking the watermark that was added to the real clip content.

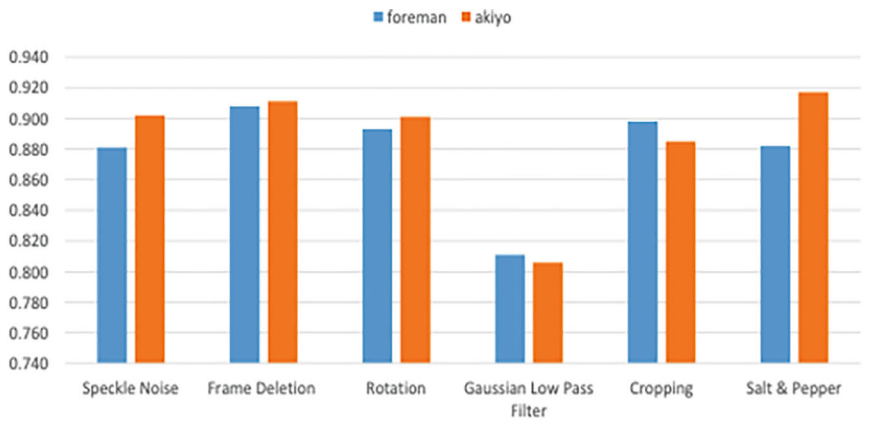

Fig. 1.7 Comparative of the foreman and Akiyo videos' results (NC values)

Table 1.1 Findings of the suggested approach security (Foreman.avi)

S. No.	Threat conducted	NC
1	Speckle noise	0.881
2	Frame deletion (around 10%)	0.908
3	Rotation	0.893
4	Gaussian low-pass filter	0.811
5	Cropping	0.898
6	Salt and pepper	0.882

Table 1.2 Proposed algorithm robustness results (akiyo.avi)

S. No.	Threat conducted	NC
1	Speckle noise	0.902
2	Frame deletion (around 10%)	0.911
3	Rotation	0.901
4	Gaussian low-pass filter	0.806
5	Cropping	0.885
6	Salt and pepper	0.917

The suggested is found to be impervious to the aforementioned threats. Finally but not least, the initial watermark is examined and removed with NC to complete the testing process. The level of resilience of the suggested strategy is depicted in the following matrix. The two clips that the suggested approach is applied to Akieyo.avi and Foreman.avi. The attacks listed above are examples of how resilient the system is (Tables 1.1 and 1.2).

1.5 Conclusion and Future Scope

The main advantage of the suggested strategy is that it is resistant to threats, especially those that target certain clips. The suggested level of safety for the operation is achieved using two separate safety levels. The original video footage is further divided into fewer pixels by jum-bledding the watermark and removing the revolving portions before uploading. The clip's clarity is enhanced once it has been included because just a small percentage of the 300 photos in the audiovisual file were actually used. When the recommended procedure is implemented and there is no discernible difference in aesthetic between these engraved and original source movies, the engraved clip concealment is considered to be good. Because the actual implanted watermark and the original media source remain accessible once the removal stage is complete, this type of resulting watermarked technique is great for commercial purposes. The improved resistance versus unresolved substance and collaborative attacks should be assessed in more detail. It is also necessary to develop techniques for watermarking videos that fall into the blind category. When blind clip watermarking is utilized, neither the source clip nor the original watermark are required to collect the incorporated watermark.
The input format for the above table is as follows:

Declarations

- Funding: No Funding
- Conflict of interest/Competing interests (check journal-specific guidelines for which heading to use): N/A
- Ethics approval and consent to participate: N/A
- Consent for publication: N/A
- Data availability: Not Publically Available
- Materials availability: No
- Code availability: Not Publically Available
- Author contribution: The Corresponding author did all the research work from data collecting writing manuscript and implementation rest of other authors assist the corresponding author.

References

1. Saxena P, Kumar S, Alam F (2023) Robust video watermarking algorithm based on motion frames and encryption. J Discrete Math Sci Cryptogr 26(5):1327–1339 (Scopus Indexed, Taylor & Francis)
2. Saxena P, Kumar S (2023) Robust video watermarking algorithm based on DCT-SVD approach and encryption. Int J Recent Innov Trends Comput Commun 11(5):85–91 (Scopus Indexed)

3. Li Q, Chang EC (2006) Zero-knowledge watermark detection resistant to ambiguity attacks. In: Proceedings of the multimedia and security workshop MM and Sec'06. https://doi.org/10.1145/1161366.116139510.1145/1161366.1161395
4. Shanmugam M, Chokkalingam A (2018) Performance analysis of 2 level DWT-SVD based non-blind and blind video watermarking using range conversion method. Microsyst Technol 24(12). https://doi.org/10.1007/s00542-018-3870-x10.1007/s00542-018-3870-x
5. Praful Saxena DSK (2019) Robust video watermarking scheme based on DWT and SVD approach using multiple frequency bands. Parishodh 8(9):10
6. Abdallah HA, Hadhoud MM, Shaalan AA (2009) SVD-based watermarking scheme in complex wavelet domain for color video. https://doi.org/10.1109/ICCES.2009.538322010.1109/ICCES.2009.5383220
7. Nouioua I, Amardjia N, Belilita S (2018) A novel blind and robust video watermarking technique in fast motion frames based on SVD and MR-SVD. Secur Commun Netw. https://doi.org/10.1155/2018/671206510.1155/2018/6712065
8. Kaur R, Jindal S (2013) Semi-blind image watermarking using high frequency band based on DWT-SVD. https://doi.org/10.1109/ICETET.2013.510.1109/ICETET.2013.5
9. Veličković ZS, Milivojević ZN, Veličković MZ (2018) A secured digital video watermarking in chrominance channel. In: 2018 23rd international scientific-professional conference on information technology, IT 2018. https://doi.org/10.1109/SPIT.2018.835085810.1109/SPIT.2018.8350858
10. Mohammed AA, Salih DA, Saeed AM, Kheder MQ (2020) An imperceptible semi-blind image watermarking scheme in DWT-SVD domain using a zigzag embedding technique. Multimed Tools Appl 79:43–44. https://doi.org/10.1007/s11042-020-09694-910.1007/s11042-020-09694-9

Chapter 2
Next-Gen Predictive Analytics: Machine Learning Transformations in Diabetes Diagnosis

Unnati Patel, Dhatri Raval, Mubina Malik, and Kalpit Soni

Abstract Diabetes, a common metabolic disorder, poses serious health risks and can lead to a variety of complications if not treated. Early detection is critical for mitigating these risks, making accurate prediction methods essential. In this study, we look at how various machine learning classifiers (KNN, Logistic Regression, Random Forest, SVM with Linear, RBF, and Polynomial Kernels, and Gradient Boosting) perform in categorizing diabetic patients. We evaluate these classifiers' performance using metrics like accuracy using data from the UCI ML repository. Furthermore, we use feature engineering techniques to preprocess and clean the data, improving the quality of input features and resulting in better model performance. Through our comparative analysis, we hope to identify optimal approaches for diabetes prediction, contributing to improved diagnosis.

Keywords Diabetes prediction · KNN algorithm · Machine learning · SVM RBF Kernel · Random Forest · Diabetes mellitus

2.1 Introduction

Diabetes is a lifelong metabolic disorder characterized by elevated blood glucose levels, which can lead to complications affecting the heart, blood vessels, kidneys, eyes, liver, and nerves. Type 2 diabetes, the most common form, primarily occurs in adults and results from either insulin resistance or insufficient insulin production. Over the past 30 years, its prevalence has increased significantly across countries with diverse socioeconomic backgrounds. Type 1 diabetes, formerly referred to as juvenile or insulin-dependent diabetes, is a chronic condition in which the pancreas produces little to no insulin [1].

U. Patel (✉) · D. Raval · M. Malik · K. Soni
Smt. Chandaben Mohanbhai Patel Institute of Computer Applications, Faculty of Computer Science and Applications, CHARUSAT, Changa, India
e-mail: unnatipatel.mca@charusat.ac.in

A. E. Hassanien et al. (eds.), *Innovative Computing and Communications*, Lecture Notes in Networks and Systems 1439, https://doi.org/10.1007/978-981-96-7137-3_2