Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 226-242
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.006

Design of Digital Image Watermarking Technique with Two Stage Vector Extraction in Transform Domain

R. Kanthavel

Department of Computer Engineering, King Khalid University, Abha, Kingdom of Saudi Arabia

E-mail: kanthavel2005@gmail.com

Abstract

Multimedia data in various forms is now readily available because of the widespread usage of Internet technology. Unauthorized individuals abuse multimedia material, for which they should not have access to, by disseminating it over several web pages, to defraud the original copyright owners. Numerous patient records have been compromised during the surge in COVID-19 incidents. Adding a watermark to any medical or defense documents is recommended since it protects the integrity of the information. This proposed work is recognized as a new unique method since an innovative technique is being implemented. The resilience of the watermarked picture is quite crucial in the context of steganography. As a result, the emphasis of this research study is on the resilience of watermarked picture methods. Moreover, the two-stage authentication for watermarking is built with key generation in the section on robust improvement. The Fast Fourier transform (FFT) is used in the entire execution process of the suggested framework in order to make computing more straightforward. With the Singular Value Decomposition (SVD) accumulation of processes, the overall suggested architecture becomes more resilient and efficient. A numerous quality metrics are utilized to find out how well the created technique is performing

ISSN: 2582-418X
Submitted: 30.08.2021
Revised: 10.10.2021
Accepted: 29.10.2021
Published: 08.11.2021

in terms of evaluation. In addition, several signal processing attacks are used to assess the effectiveness of the watermarking strategy.

Keywords: Digital watermarking, Fast Fourier Transform, robust, security, copyright protection, singular value decomposition

1. Introduction

A partial answer to the copyright ownership dilemma is digital watermarking. Sideband data embedding directly into digital audio, picture, or video samples is known as watermarking. Besides the digital signal itself, sideband data may include things like block headers or time synchronisation markers that must be sent along with it. The watermark is not an add-on by the digital data but is a part of the image itself. A digital data is generated in multiple formats and the originality may be lost during various attacks, though the samples of digital information are static features. This is where watermarking comes in handy [1-6].

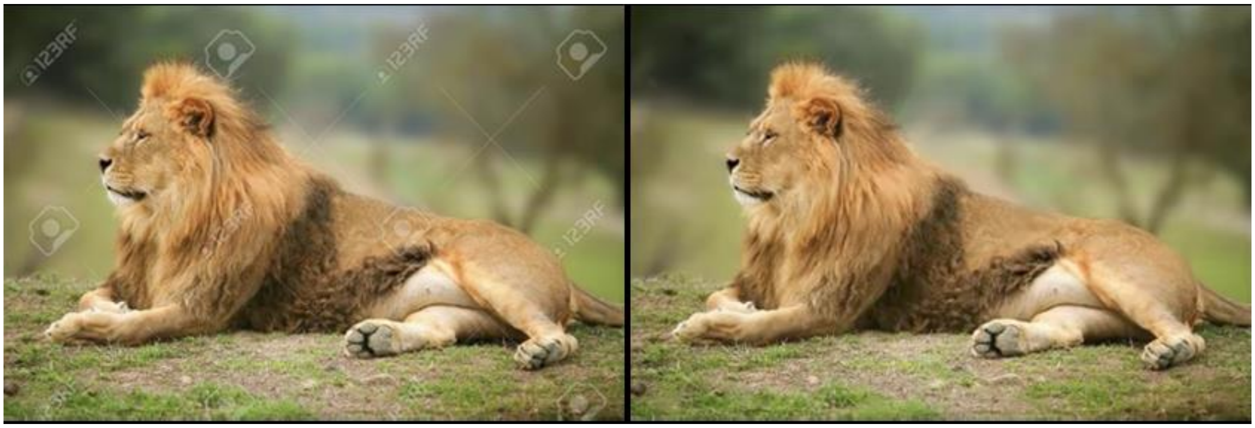

Figure 1. Visible and invisible watermarking

Modern and inexpensive digital watermarking contains the recording unit with storage capacity to build a platform to access many multimedia content in digital formats without altering

ISSN: 2582-418X
Submitted: 30.08.2021
Revised: 10.10.2021
Accepted: 29.10.2021
Published: 08.11.2021

the quality of images [7, 8]. General-purpose PCs and graphics editing software are adequate resources needed for a person without a lot of expertise or professional talents to start with. The visible and invisible watermarking sample images are shown in figure 1.

There are no discernible traces left behind when it manipulates or tampers a picture, bringing out the best in digital photographs and recreating them into whatever a person wishes for. Researchers, scientists, and practising engineers in the multimedia publishing industries place a high value on pervasive advances because unauthorised person details of original multimedia data can be spread through many communication channels such as guided or unguided media [9-12].

Encoders and decoders are the most common parts of digital watermarking systems. They use cover media data and watermark encoder as input and an embedding security key as output. There are numerous methods for incorporating machine-readable code into digital media such as music, video, and images. The encoder modifies the material to enter the machine-readable code and then retrieve it in a way that ensures basic security while extracting watermark information. The simplified procedure of watermarking method is shown in figure 2.

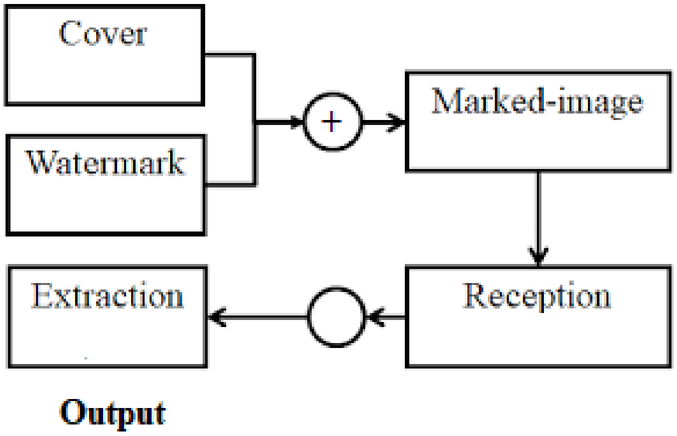

Figure 2. Simplified work for watermarking procedure

Consequently, the necessity for appropriate solutions to assure tamper resistance and avoid digital content owners' harm is critical. Digital multimedia data's copyright and intellectual property should be guarded against unauthorised ownership, replication, and distribution due to potential copyright difficulties. Encryption, steganography, and watermarking are all new approaches being introduced [13-15]. Not all watermarking methods have the same amount of resilience. It depends on the application. While some can withstand a variety of image processing assaults, others are vulnerable. As a result, three levels of robustness exist: strong, fragile, and semi-fragile.

2. Preliminaries

A recent proposal by Wazid et al. presents lightweight authentication mechanism in a cloud-based IoT environment that allows authenticated persons to access the data. Researchers have shown enhanced security using security based encryption function with gate operation [16].

Singh et al. introduced telemedicine hybrid domain based watermarking method. A DWT-SVD-based watermarking approach embeds dual function such as image and text that are incorporated within the image. Text watermarks are made more resilient by using four error correction codes (ECCs) throughout the embedding and extraction procedures [17].

SVD and the redundant discrete wavelet transform were combined with a hybrid resilient watermarking approach suggested by Roy and Pal to protect the copyright of color photographs [18]. Using entropy and QR decomposition, Laur et al. introduced a resilient color picture watermark in their research. Selecting image blocks for watermark embedding was done using entropy. The data can be embedded into a single value of the image after the transform with SVD [19].

ISSN: 2582-418X
Submitted: 30.08.2021
Revised: 10.10.2021
Accepted: 29.10.2021
Published: 08.11.2021

According to Mishra et al. various scale parameters affect the imperceptibility and resilience of watermarks. They developed an improved SVD-based watermarking approach, which uses an optimization process known as the firefly algorithm to identify the appropriate scaling factor [20].

The Discrete Wavelet Transform (DWT) is most likely to be used for embedding watermarks in digital images going forward. Due to DWT's reputation as a trustworthy transformation method, many scientists have used it. On the other hand, the smallest bit modification technique is insufficient to protect against certain signal processing threats. It's no secret that frequency-domain approaches like DCT and DWT are popular among scientists. These approaches have been merged into one termed singular value decomposition since the forms often confront issues like matrix dimensionality reduction [21].

There may be huge difficulties in the process of watermarking even though this technique provides a fair balance between robustness and imperceptibility. SVD and the integer wavelet transform were combined by Makbol and Khoo [22] to create a false-positive-free watermarking technique. The identification print details from the matrix U and V is placed for the orthogonal function to avoid the false positive situation. A certification procedure is carried out before watermark extraction at the time of watermark predication. The authentication is extracted from the image at initial stage. Ansari et al. presented the procedure to improve the robust and reliability of the watermarked image against various attacks [23].

3. Methodologies

In digital picture watermarking systems, robustness is prerequisite for the detection of a watermark after typical signal processing modification operations are performed. The process includes mapping, filtering an zigzag scanning procedure and compression after scaling transfer

ISSN: 2582-418X
Submitted: 30.08.2021
Revised: 10.10.2021
Accepted: 29.10.2021
Published: 08.11.2021

function. Additionally, they encompass various processes, such as analog-to-digital conversion, digital-to-analog conversion, picture enhancement, cutting, and so on [24-26].

3.1 Proposed scheme

This portion of the research paper describes the suggested approach, which is based on FFT and SVD. The process consists of two parts. "Watermark generation and extraction" are the terms used to describe the specific action that will be described in the next subsections. Figure 3 & 4 shows the proposed methodology.

3.2 Watermark Generation

Step 1: The FFT decomposition is done first on the carrier image, which yields the frequency domain and reduces processing complexity.

Step 2: To minimise the impact of watermark generation, two identical watermarks are inserted in different frequency sub-bands. The block based SVD can be applied into each and every block that is generated by splitting the picture into 16*16 blocks, using the other band frequencies as an example.

Step 3: A dual orthogonal matrix, designated by M, is generated using the direct coefficient of each sub-block. Singular values of the matrix M may be found using the below equation, which is applied to the coefficient matrix.

$$M = USV^T$$

M is equivalent to orthogonal matrices that are indicated with diagonal matrix.

Step 4: SVD is applied on S_m and the coefficient matrix M is changed. The HL sub-band embedded with a watermark is produced after the inverse transform.

ISSN: 2582-418X
Submitted: 30.08.2021
Revised: 10.10.2021
Accepted: 29.10.2021
Published: 08.11.2021

$$S_m = S + a * W_1$$

Step 5: In order to add the second stage watermark to the other sub-band, the same procedure is used.

Step 6: Carrier images are watermarked using the inverse DIF (Decimation In Frequency) method.

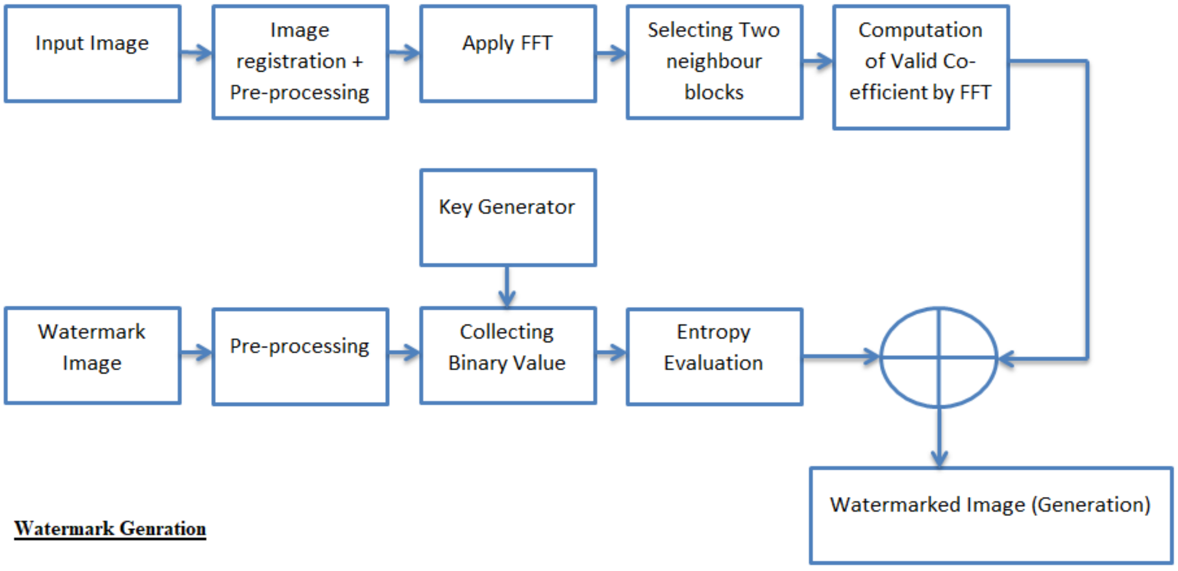
Input Image
Image registration + Pre-processing
Apply FFT
Selecting Two neighbour blocks
Computation of Valid Co-efficient by FFT
Key Generator
Watermark Image
Pre-processing
Collecting Binary Value
Entropy Evaluation
Watermarked Image (Generation)
Watermark Genration

Figure 3. Proposed watermark procedure / algorithm

3.3 Watermark extraction

Step 7: FFT alters the received picture, which may have been corrupted as a result of several assaults. Afterwards, various band frequency characteristics are gathered.

Step 8: The various band images are segmented into 16*16 blocks for computation in order to retrieve the watermark from all the sub-bands of the given image. On each sub-block, the SVD

ISSN: 2582-418X
Submitted: 30.08.2021
Revised: 10.10.2021
Accepted: 29.10.2021
Published: 08.11.2021

is carried out using the same algorithm. When all of these factors are added together, a new matrix, M, is created.

Step 9: The SVD is used to convert the newly created matrix M into three new matrices as shown in the below equation.

$$M^* = U^* S^* (V^*)^T$$

The same procedure is used to produce the second watermark. Lastly, the average of these two watermarks is used to calculate the watermark, W.

Correctness:

A sign function is used to adjust the watermark to maximize the quality of the images with watermarked content that is defined as,

$$W^*(i,j) = \begin{cases} 1\, W(i,j) \geq T, \\ 0, W(i,j) < T \end{cases}$$

where T is the desired threshold value.

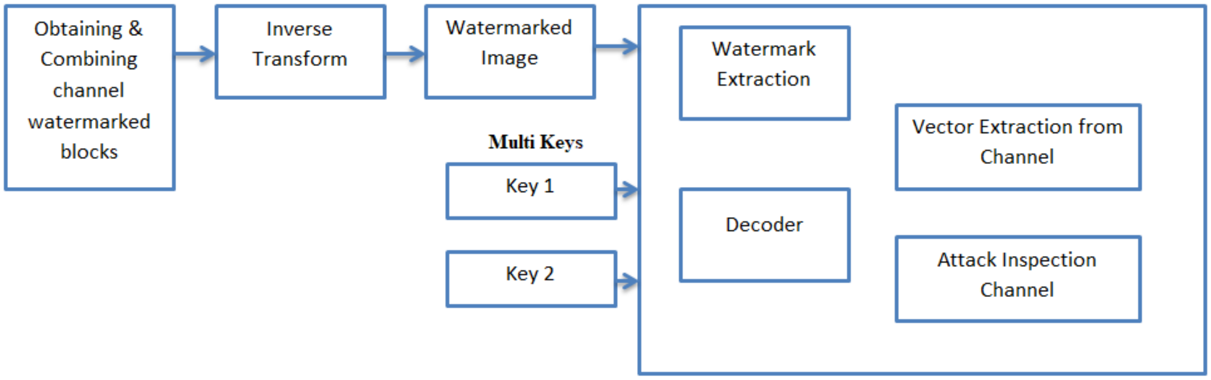
Obtaining & Combining channel watermarked blocks
Inverse Transform
Watermarked Image
Multi Keys
Key 1
Key 2
Watermark Extraction
Vector Extraction from Channel
Decoder
Attack Inspection Channel

Figure 4. Second stage of proposed watermarking extraction algorithm flow

ISSN: 2582-418X
Submitted: 30.08.2021
Revised: 10.10.2021
Accepted: 29.10.2021
Published: 08.11.2021

To achieve high resilience, there are numerous broadways, including redundant embedding, spread spectrum, and embedding watermarks. To ensure that watermark data can't be removed or omitted by unauthorized distributors, a suitable digital watermarking system must withstand multiple attacks.

4. Results and discussion

Evaluation indicators such as Bit Error Rate (BER), Normalized Correlation (NC), Structural Similarity Index Measure (SSIM), and Peak signal to Noise Ratio (PSNR) are used to assess the effectiveness of the method. PSNR is a powerful statistic for determining whether a photograph is watermarked or not, based on the image's mean square error value. Here the BER is nothing but reciprocal of PSNR value [27-30]. These settings establish a connection between the watermarked picture and the original one.

$$PSNR = 10 * \log\left(\frac{255^2}{MSE}\right)$$

$$NC = \frac{\sum_{i=1}^{32}\sum_{j=1}^{32} W_1(i,j) * W^*(i,j)}{\sum_{i=1}^{32}\sum_{i=1}^{32} W_1(i,j) * W_1(i,j)}$$

The first two photos (a and b) are shown in the customary way. The suggested work is shown in Figure 5c. When the attack takes place, the resilience of the other conventional techniques are tested at the location of the watermarked insertion, as seen in figure 5.

The created algorithm's efficiency is solely determined by the quality measures whose values are acquired. To compare the two images, all quality metrics must be distinguished between the original and the watermarked version. The PSNR performance graph is shown in figure 6.

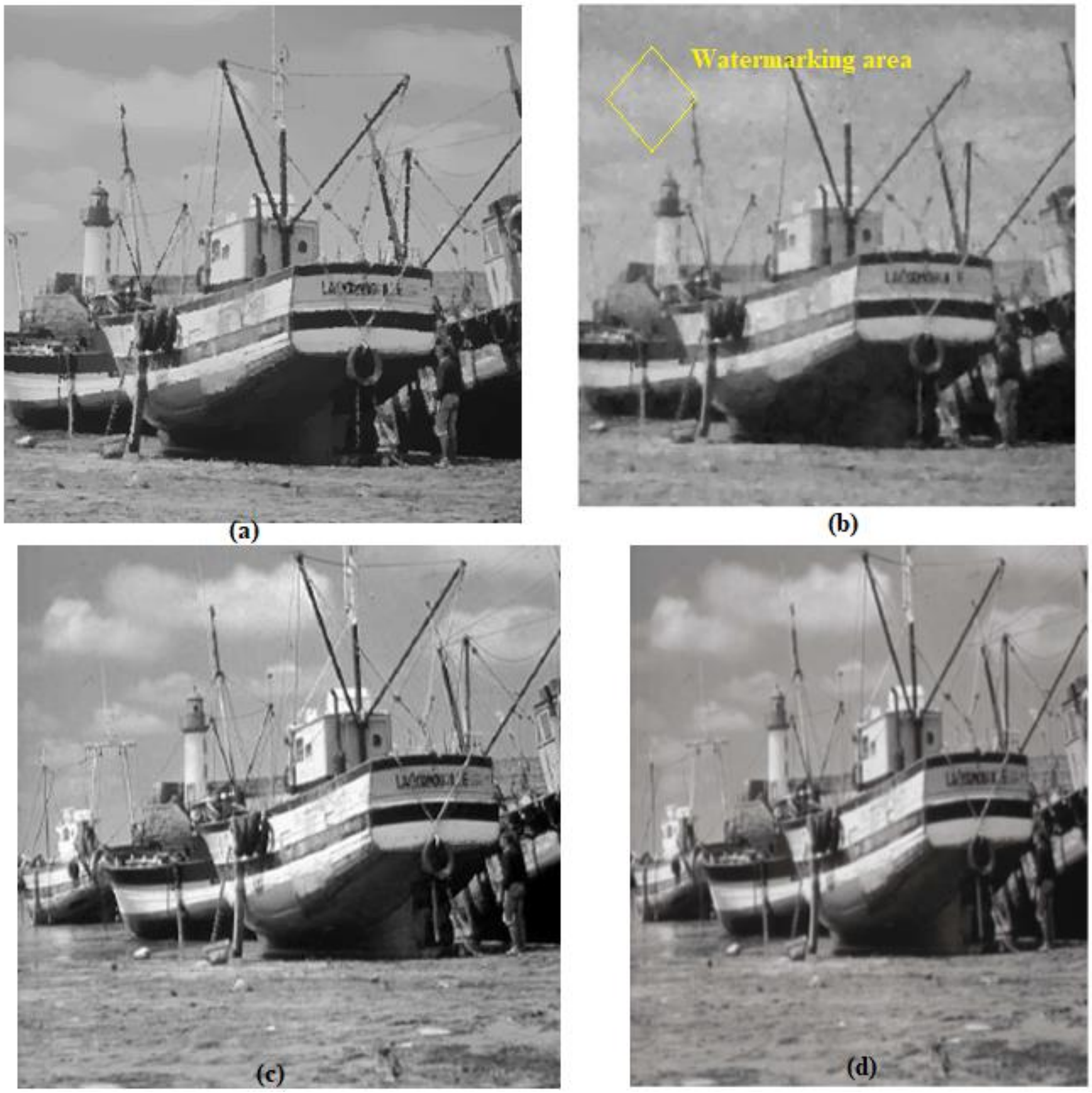

Figure 5. Obtained resultant of robust watermark images

There are several noise-based and geometric-based attacks that can be prevented by a watermark that does not modify the watermark data. After various assaults, the watermark stays the same and authenticates the user by detecting the watermark [30-33].

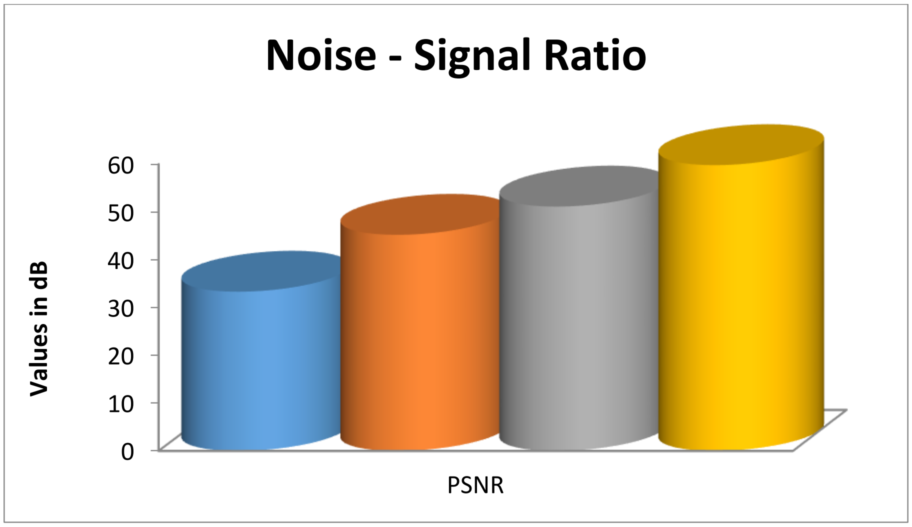

Figure 6. PSNR performance of proposed framework

Using bit error rate as an estimate, the quality parameter is utilised in the research work. Both invisibility and embedding time are used to evaluate how well the procedure works. Over the years, several scientists have worked to improve on already-developed processes. Table 1 containes the computed performance metrics of various algorithms.

Table 1. Computed performance metrics for proposed algorithm

Method	**Bit Error Rate**	**Normalized Co-efficient**	**PSNR**	**SSIM**	**Overall Robust**	**Computation Time (Sec)**
WT	0.03	0.5313	33.31	0.7854	Low	6.21
DCT+FFT	0.022	0.8671	45.21	0.8879	Moderate	4.43
DWT+SVD	0.0195	0.8723	51.12	0.9103	High	7.78
Proposed FFT + SVD	0.016	0.9711	59.79	0.9807	High	4.15(speedy)

ISSN: 2582-418X
Submitted: 30.08.2021
Revised: 10.10.2021
Accepted: 29.10.2021
Published: 08.11.2021

Here, the suggested method is compared to what has already been discovered over time. Based on embedding time and quality measures, Table 1 compares the proposed method with other different approaches. Figure 7 shows NC and SSIM performance chart for various methods.

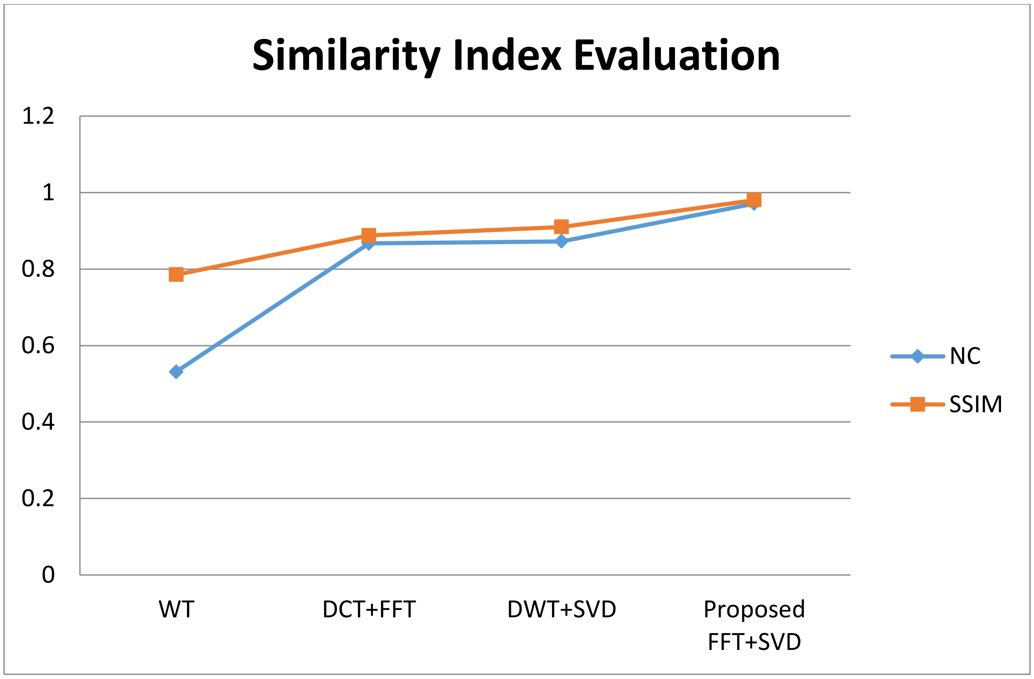

Figure 7. NC & SSIM computation chart

Depending on the task, each researcher has employed a unique collection of natural images from a created dataset. It is impossible to compare the suggested method's performance to current methods by using quality criteria to evaluate its performance by computation time (speedy). When comparing the proposed approach to current practices, embedding time becomes critical. Different sets of pictures are used for the comparison study, and the estimate of embedding time is determined to the nearest second in seconds [34]. As a result, various photographs have varying results when it comes to watermarking. The suggested method's efficiency is determined by the embedding time which is deduced based on the findings in Table 1.

ISSN: 2582-418X
Submitted: 30.08.2021
Revised: 10.10.2021
Accepted: 29.10.2021
Published: 08.11.2021

5. Conclusion

As a result, the suggested framework outperforms the competition in terms of attack performance owing to its novel and creative structure for resilience. The algorithm that demonstrated the high efficiency of the framework is used to determine the performance metrics for the method. When compared to other standard methods, the proposed methodology is much faster during execution as shown in table 1. The suggested technique, however, faces the issue of false positives, which is still an open question. This problem will be addressed in the future, and the suggested solution will be applied to colour photos as well. For imperceptible resilience and increased data embedding capacity, it is essential that image data be secure. For these reasons, hybrid digital picture watermarking is an important area of study. The present hybrid approach, on the other hand, need improvement, on how IoT based authentication can be enhanced further with watermarking images. Further study will incorporate machine learning with various neural networks that can be implemented in the wavelet transform domain to promote resilience and security based word embedding procedure.

References

[1] Manoharan, J. Samuel. "A Novel User Layer Cloud Security Model based on Chaotic Arnold Transformation using Fingerprint Biometric Traits." Journal of Innovative Image Processing (JIIP) 3, no. 01 (2021): 36-51.

[2] M. Dehghani, Z. Montazeri, O. Malik, G. Dhiman, and V. Kumar, “BOSA: binary orientation search algorithm,” International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 1, 2019.

[3] Sharma, Rajesh, and Akey Sungheetha. "An Efficient Dimension Reduction based Fusion of CNN and SVM Model for Detection of Abnormal Incident in Video Surveillance." Journal of Soft Computing Paradigm (JSCP) 3, no. 02 (2021): 55-69.

ISSN: 2582-418X
Submitted: 30.08.2021
Revised: 10.10.2021
Accepted: 29.10.2021
Published: 08.11.2021

[4] P. Khare and V. Srivastava, “A secured and robust medical image watermarking approach for protecting integrity of medical images,” Transactions on Emerging Telecommunications Technologies, vol. 32, no. 2, 2021.

[5] Kumar, T. Senthil. "Video based Traffic Forecasting using Convolution Neural Network Model and Transfer Learning Techniques." Journal of Innovative Image Processing (JIIP) 2, no. 03 (2020): 128-134.

[6] A. Sharma, B. Bagga, M. S. Singh, and M. Shabaz, “A novel optimized graph-based transform watermarking technique to address security issues in real-time application,” Mathematical Problems in Engineering, vol. 2021, 27 pages, 2021.

[7] Manoharan, J. Samuel. "Capsule Network Algorithm for Performance Optimization of Text Classification." Journal of Soft Computing Paradigm (JSCP) 3, no. 01 (2021): 1-9.

[8] H. Egilmez, Y. Hsuan, and C. Ortega, “Graph-based transforms for video coding,” in IEEE Transactions on Image Processing, vol. 29, pp. 9330–9344, Kyoto, Japan, September 2020.

[9] Manoharan, J. Samuel. "Study of Variants of Extreme Learning Machine (ELM) Brands and its Performance Measure on Classification Algorithm." Journal of Soft Computing Paradigm (JSCP) 3, no. 02 (2021): 83-95.

[10] W. Wang, H. Y. Tan, P. Sun, Y. Pang, and B. B. Ren, “A novel digital image encryption algorithm based on wavelet transform and multi-chaos,” Wireless Communication and Sensor Network, pp. 711–719, 2016.

[11] Pandian, A. Pasumpon. "Artificial intelligence application in smart warehousing environment for automated logistics." Journal of Artificial Intelligence 1, no. 02 (2019): 63-72.

[12] Z. Cao and L. Wang, “A secure video watermarking technique based on hyperchaotic Lorentz system,” Multimedia Tools and Applications, vol. 78, no. 18, pp. 26089–26109, 2019.

[13] Hamdan, Yasir Babiker, and A. Sathesh. "Construction of Efficient Smart Voting Machine with Liveness Detection Module." Journal of Innovative Image Processing 3, no. 3 (2021): 255-268.

[14] W. Wang, M. M. Si, Y. Pang et al., “An encryption algorithm based on combined chaos in body area networks,” Computers and Electrical Engineering, vol. 65, pp. 282–291, 2018.

[15] Vijayakumar, T., Mr R. Vinothkanna, and M. Duraipandian. "Fusion based Feature Extraction Analysis of ECG Signal Interpretation–A Systematic Approach." Journal of Artificial Intelligence 3, no. 01 (2021): 1-16.

[16] M. Wazid, A. K. Das, K. Vivekananda Bhat, and A. V. Vasilakos, “LAM-CIoT: lightweight authentication mechanism in cloud-based IoT environment,” *Journal of Network and Computer Applications*, vol. 150, Article ID 102496, 2020.

[17] Singh, A.K.; Kumar, B.; Dave, M.; Mohan, A. Robust and imperceptible dual watermarking for telemedicine applications. Wirel. Pers. Commun. **2015**, 80, 1415–1433.

[18] Roy, S.; Pal, A.K. An SVD based location specific robust color image watermarking scheme using RDWT and Arnold Scrambling. Wirel. Pers. Commun. **2018**, 98, 2223–2250.

[19] Laur, L.; Rasti, P.; Agoyi, M.; Anbarjafari, G. A robust color image watermarking scheme using entropy and QR decomposition. Radioengineering **2015**, 24, 1025–1032.

[20] Mishra, A.; Agarwal, C.; Sharma, A.; Bedi, P. Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm. Expert Syst. Appl. **2014**, 41, 7858–7867.

[21] Ali, M.; Ahn, C.W. Comments on “Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm”. Expert Syst. Appl. **2015**, 42, 2392–2394.

[22] Makbol, N.M.; Khoo, B.E. A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. Digital Signal Process. **2014**, 33, 134–147.

[23] Ansari, I.A.; Pant, M.; Ahn, C.W. Robust and false positive free watermarking in IWT domain using SVD and ABC. Eng. Appl. Artif. Intell. **2016**, 49, 114–125.

[24] C. Sharma and A. Bagga, “Video watermarking scheme based on DWT, SVD, rail fence for quality loss of data,” in 2018 4th International Conference on Computing Sciences (ICCS), pp. 84–87, Jalandhar, India, August 2018.

[25] Sathesh, A., and Edriss Eisa Babikir Adam. "Hybrid Parallel Image Processing Algorithm for Binary Images with Image Thinning Technique." Journal of Artificial Intelligence 3, no. 03 (2021): 243-258.

[26] C. Sharma, B. Amandeep, R. Sobti, T. Lohani, and M. Shabaz, “A secured frame selection based video watermarking technique to address quality loss of data: combining graph based transform, singular valued decomposition, and hyperchaotic encryption,” Security and Communication Networks, vol. 2021, 19 pages, 2021.

[27] Vijayakumar, T. "Synthesis of Palm Print in Feature Fusion Techniques for Multimodal Biometric Recognition System Online Signature." Journal of Innovative Image Processing (JIIP) 3, no. 02 (2021): 131-143.

[28] F. Ajaz, M. Naseem, S. Sharma, M. Shabaz, and G. Dhiman, “COVID-19: challenges and its technological solutions using IoT,” Current Medical Imaging, vol. 17, 2021.

[29] Manoharan, J. Samuel. "Capsule Network Algorithm for Performance Optimization of Text Classification." Journal of Soft Computing Paradigm (JSCP) 3, no. 01 (2021): 1-9.

[30] Kumar, Parmalik, and A. K. Sharma. "A robust digital image watermarking technique against geometrical attacks using support vector machine and glowworm optimization." In International Conference on Intelligent Data Communication Technologies and Internet of Things, pp. 733-747. Springer, Cham, 2019.

[31] Sana, Ehtesham, Sameena Naaz, and Iffat Rehman Ansari. "Development of DWT–SVD based Digital Image Watermarking for Multi-level Decomposition." In Proceedings of International Conference on Intelligent Computing, Information and Control Systems, pp. 67-81. Springer, Singapore, 2021.

[32] Umapriya, A., and P. Nagarajan. "Transmission of Watermarked Image in WSN Using ELSM Algorithm." In Inventive Communication and Computational Technologies, pp. 1171-1178. Springer, Singapore, 2020.

[33] Vemuri, Sreya, and Rejo Mathew. "A Comparison Between Robust Image Encryption and Watermarking Methods for Digital Image Protection." In International conference on Computer Networks, Big data and IoT, pp. 128-138. Springer, Cham, 2019.

[34] Ananth, C., M. Karthikeyan, and N. Mohananthini. "Discrete Wavelet Transform Based Multiple Watermarking for Digital Images Using Back-Propagation Neural Network." In International Conference on Inventive Computation Technologies, pp. 441-449. Springer, Cham, 2019.

Author's biography

R. Kanthavel is a Professor in the Department of Computer Engineering at King Khalid University, Abha, Kingdom of Saudi Arabia. His research is mainly focused on the emerging smart computing technologies that includes Distributed Computing, quantum computers, computer graphics, computer networks, and web technologies.

ISSN: 2582-418X
Submitted: 30.08.2021
Revised: 10.10.2021
Accepted: 29.10.2021
Published: 08.11.2021