Robust Video Watermarking Using Bacteria Foraging Optimization

Ranjan K. Senapati(✉), P. Bhavya Reddy, K. Thirumalesh, and E. Vamshi Krishna

Department of ECE, VNR VJIET, Hyderabad, Telangana, India
ranjan_ks@vnrvjiet.in, bhavyareddy759@gmail.com,
thirumalesh6723@gmail.com, erramvamshi123@gmail.com

Abstract. Multimedia privacy is a significant issue in secret communication and copyright protection. There is always a trade-off between the quality of the information that can be extracted (watermark) and quality of the covered image/video. This study presents a novel technique for determining the ideal scaling factor in video watermarking to provide the best trade-off between the covered video and extracted watermark. The proposed approach uses the bacterial foraging optimization algorithm (BFO) to select an improved scale factor based on the BFO fitness function. The BFO fit-ness function is the reciprocal of the normalized cross correlation of the attacked video's linear combination. Singular value decomposition (SVD) and Redundant discrete wavelet transform (RDWT) are coupled to embed the watermark in video, and an inverse procedure is used to retrieve the watermark. First, the key frames are extracted from the cover video, followed by the strengthened embedding is applied to 1 level RDWT sub bands of extracted key frames. The main element of watermark is added to the RDWT sub-band. The exposition of the suggested tactic is evaluated on Normalized correlation coefficient (NNC), the image fidelity (in SSIM sense) and the PSNR to demonstrate its better functionality.

Keywords: Bacterial foraging optimization · Singular value decomposition · Redundant discrete wavelet transform

1 Introduction

Multimedia covers a major aspect of our daily lives. The transmission and protection of information content using internet needs data security. Yet, anybody with access to current technologies and the internet may change, adapt, and utilize the multimedia contents. This compels the need for researchers to improve the data security techniques. Several techniques have been evolved that can deal efficiently the concerns around ownership verification and copyright protection. One method for dealing with content authorisation and copy right protection is digital video/image watermarking. In this approach, a concealed message (i.e., watermark), such as a symbol or covert picture, is placed in the host frame in such a way that it can be quickly retrieved on the receiving side, without damaging the calibre of the original frame and watermark. Two key requirements must be met in this regard. i) Imperceptibility of the embedded watermark; and ii)

B. Raj et al. (Eds.): ICETE 2023, AER 223, pp. 873–881, 2023.
https://doi.org/10.2991/978-94-6463-252-1_88

Robustness in the face of various challenges. Robustness provides a general impression of the sustainability of algorithm under many attacks like Noise, geometric, and compression and combination attacks. Imperceptibility expresses about the general nature of the watermarked framework. Numerous algorithms have been dealing with trade-offs between imperceptibility and robustness [1–12]. Spatial domain and transform domain watermarking approaches are categorized in accordance with these limitations.

These solutions are more resistant to affine transform and typical image processing assaults. The discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), singular value decomposition (SVD), discrete tchebichef transform (DTT), and finite-rank iterative transform are the most often utilized transform domain methods (Finite ridge let transform). Several research advocated using a watermarking with amalgam approach that includes more than two transformations to boost robustness and imperceptibility.

2 Related Work

These lines mostly highlight the accompanying work done for video watermarking, as well as its merits and downsides. Hsiang-Cheh Huang et al. [1] devised a process known as DCT-based Robust Watermarking using Concepts for Swarm Intelligence. The BF algorithm was utilized in conjunction with a standard DCT-based system in this technique. Against many attacks, this algorithm performs better. Sadik Yildiz, et al. [2], DWT, DCT, and SVD-based hybrid watermarking technique is suggested, to stop copyright infractions and digital privacy violations in photographs. “Gaussian”, “shot”, “salt & pepper” and “speckle” Images that have been watermarked have noise added to them. After addition of noise, the watermarked image’s original and watermark have been retrieved. The BFO approach has been used to re-extract the original image and watermark from the optimized watermarked image. The PSO algorithm was employed in this stage to determine the ideal location for the BFO method’s chemotactic parameters. To determine how well watermarking and optimization strategies perform, PSNR, NCC, and IF values have been computed and compared. Elham Moeinaddini, et al. [3] use a combination of the distinct discrete firefly algorithm (DDFA) and entropy to pick appropriate blocks in a unique robust picture watermarking system that strikes a compromise between transparency and robustness. The robustness of this system is tested using different distinct attacks, and the findings show that it is more robust and transparent than previous similar schemes. V. Santhi et al. [4] applied Hadamard transformation technique. A full image or pattern can be concealed as a watermark within the original image. The image quality must be retained. A few blocks from the image are used for embedding, depending on the size of the watermark and the information included in each block. Cover picture is transformed from the spatial domain to the transform domain using the Hadamard transformation to lower the computational cost of the suggested approach. A reliable discrete wavelet transform (DWT)-based singular value decomposition (SVD) and human visual system watermarking technique is suggested by Nasrin M. Makbol et al. [5]. It is basically a block-based scheme that makes use of edge entropy and entropy as HVS features for choosing relevant blocks in which to place the watermark. The blocks with the lowest edge and block entropy values are chosen as the finest places to place the watermark. This approach demonstrated remarkable robustness and imperceptibility against all image-processing attacks as well as a number of geometrical attacks.

Xiaobing Gan, et al. [6] mentioned that the traditional BFO method has some potential flaws, including weak precision of convergence and absence of swarm communication. Due to the resolution of these problems, an enhanced BFO algorithm with extensive swarm learning techniques (LPCBFO) is developed.

Divya et al. [7] used RDWT with SVD scheme for eliminating geometrical attacks. Charu Agarwal et al. [8] DWT-SVD and the fire-fly algorithm were used to suggest an improved method of watermarking grayscale images A binary watermark's values are anchored in the singular values of the cover image's LL3 sub-band utilizing several scale factors. The method performs well when tested against several image processing assaults and the false positive detection issue is eliminated. Amir wagdarikar et al. [9] employed a fitness function with a range of inputs, such as brightness, wavelet energy, and pixel intensity.These features were taken from the cover video and passed into the chronology-MS algorithm, which chooses the best locations to place the watermark. In every spec, this algorithm outperformed others. C. Priya et al. [10] established a powerful and safe video watermarking method relying on "Cellular Automata and SVD for Copyright Protection". A mix of cell automata and SVD is used in the strategic approach. This guarantees copyright and provides indistinctness for many change planes. An method for video steganography proposed by Meenu Suresh et al. [11] employs Fractional Grey Wolf Optimization and a cost function with many objectives. Using an estimation of the Structural Similarity Index (SSIM), the Key Frames are selected. The cost function may include energy, coverage, intensity and kurtosis selects the optimal regions. Ranjan K. Senapati et al. [12] proposed and RST invariant watermarking scheme which provide robust against all possible attacks. The scheme is similar to the scheme as in [7]. The difference is the transform.

Bacterial Foraging Optimization: BFO algorithm is a Nature Inspired Optimization Algorithm, this process is stimulated by Foraging behavior of Escherichia (i.e., E. Coli) Bacteria. The fundamental science underlying E. coli's scavenging process is highlighted in a peculiar manner and used as an unassuming enhancement calculation. BFO can usually have four stages i.e., Chemotaxis, Swarming, Reproduction and Elimination and dispersal. The proposed scheme uses BFO for finding optimum scale factor (β).

3 Methods and Models

In the subsection that follows, the suggested calculation for installing and extracting watermarks is explained. It combines the SVD, RDWT and BFO algorithms. Before being placed into one of RDWT's sub-bands, the watermark image is randomly reconfigured. This will provide an additional layer of security to the proposed approach. Figure 1 depicts a graphic representation of the proposed scheme.

3.1 Key Frame Extraction

The host video has many frames, so key frames are chosen based on minimum entropy criteria. This ensures the increased robustness of the system. Assume F is the number of

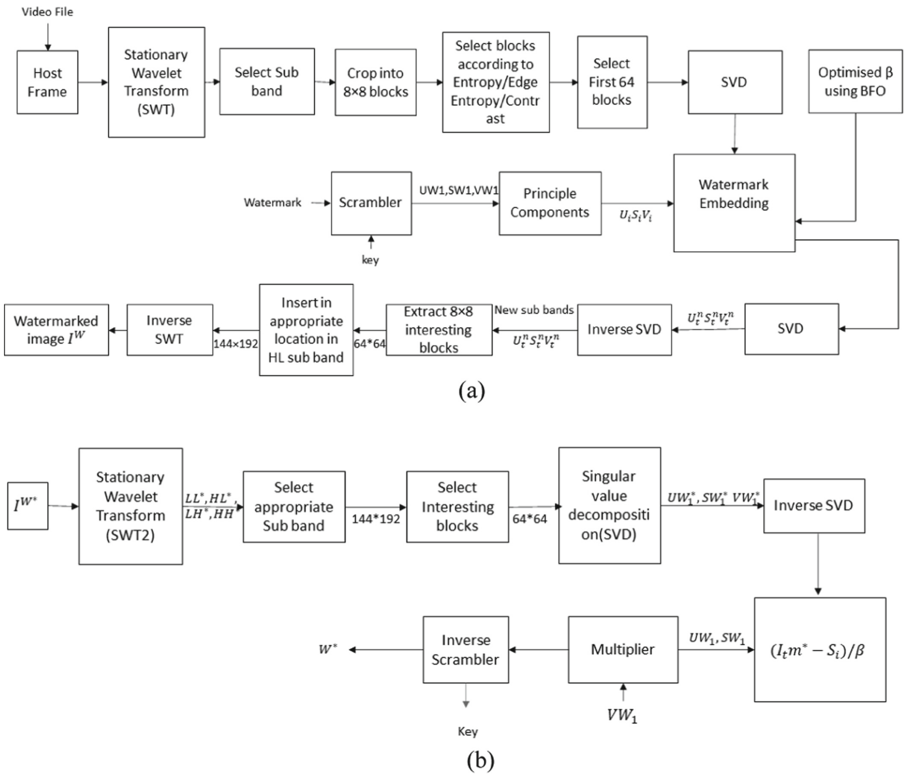


Fig. 1. Suggested scheme block diagram of (a) embedding and (b) extraction process

viewable frames in a movie, and we want to use F/n to identify critical frames, where n is the integer value. So,

$$Key\ Frames = \{Y_q, 1 \leq q \leq F\} \tag{1}$$

3.2 BFO (Bacterial Foraging Optimization)

Initialize the BFO parameters such as, p = dimension of search space, s = the number of bacterium, N_c = Chemotactic steps, N_{re} = The reproduction steps number, N_{ed} = The elimination and dispersal steps, S_r = The bacteria reproductions (splits) per generation number, Ped = probability of elimination, C(i) = step size. For our experiment, we used the following values for all of the parameters:

{p = 4, s = 6, N_c = 2, N_s = 2, N_{re} = 1, N_{ed} = one, S_r = s/2, Ped = 0.25, C(i) = 0.05*ones (s,1)}.

3.3 Redundant Discrete Wavelet Transform

The DWT has many drawbacks. The primary drawback is the shift invariant property. This is because each level of filtering is followed by a down-sampling procedure, which alters the image's wavelet coefficients significantly even after a small shift. The result is inaccurate reconstruction of watermark data and cover image. RDWT resolves the shift invariant property of DWT [13].

3.4 Embedding Algorithm

The proposed scheme's embedding phase involves the following steps,

1. Select the key frames from cover video.
2. Apply the RDWT on key frame selected. Select HH Sub-band and crop the subband to 8 × 8 blocks.
3. Select blocks according to a predefined criteria and apply SVD on to it.

$$\{U_i, S_i, V_i\} = SVD(HH3) \tag{2}$$

4. Select the watermark image (W), then apply SVD and permutation on it.

$$\{uw_1, sw_1, vw_1\} = SVD(W) \tag{3}$$

5. Use BFO to identify the optimal scaling factor.
6. Embed the watermark in cover object's S plane by using the following equation.

$$S_i^{WT} = S_i + \beta.(uw_1 \times sw_1) \tag{4}$$

7. Apply SVD on modified coefficients of S_i^{WT}

$$\left\{U_i^n, S_i^n, V_i^{nT}\right\} = SVD(S_i^{WT}) \tag{5}$$

8. Apply inverse SVD with singular coefficients using the equation below.

$$I^{WT} = U_i S_i^n V_i^T \tag{6}$$

9. Extract 8 × 8 blocks and insert the block locations in HH subbands.
10. Reconstruct the final HH subband and do inverse RDWT to reconstruct the watermarked video frame.

3.5 Extraction Algorithm

The extraction phase of the proposed technique involves the following processes,

1. Select the key frames. Apply RDWT to the watermark key frame that was attacked and select the tampered/attacked sub-bands like .

$$\{LL_3^{w^*}, HL_3^{w^*}, LH_3^{w^*}, HH_3^{w^*}\}$$

2. Select the appropriate subband. Select the blocks according to predefined criteria as mentioned. Apply SVD on attacked $LL_3^{w^*}$ sub-band according to the Eq. (7).

$$I_i^{n^*} = U_i^{n^*}.S_i^{w^*}.V_i^{n^*} \tag{7}$$

3. Apply inverse SVD on $S_i^{w^*}$, while keeping U_i^n & V_i^n obtained from Eq. (7) used as embedding keys from embedding phase. So,

$$I_i^{n^*} = U_i^n S_i^{w^*} V_i^n \tag{8}$$

4. Now, apply the below formula to remove the watermark,

$$WT_{extrxct} = \frac{I_i^{n^*} - S_i}{\beta} \tag{9}$$

$$WT_{extract}^{*} = WT_{extrxct} \times vw_1^T \tag{10}$$

5. Apply the inverse permutation/hash to the watermark in (10) to get the final watermark.

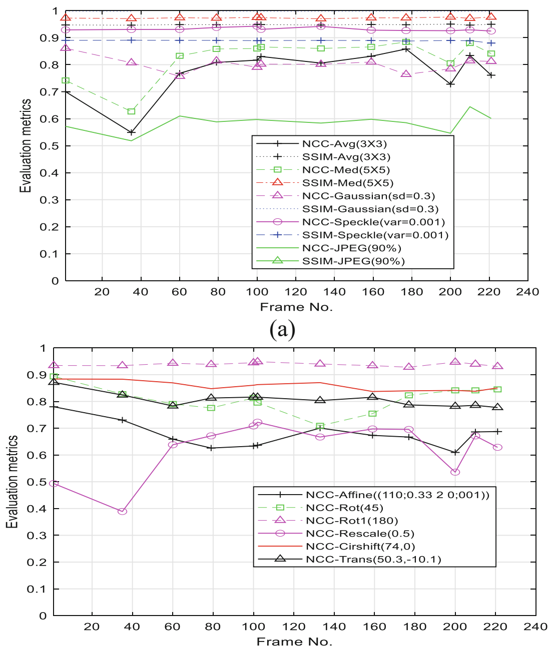
4 Results and Analysis

The algorithm simulation is carried out on a MATLAB 2022a platform using i5 CPU, 16GB RAM computer.

The test results for video watermarking utilizing RDWT + BFO + SVD appeared is applied to the embedding and extraction scheme shown in Fig. 1. Figure 2 shows the NCC and SSIM performance of the method at different frames. Each selected frames are the frames with minimum entropy among a group of 20 frames (e.g., min. Entropy frames from 0–20, 21–40, 41–60 and so on). Figure 2(a) shows the imperceptibility and robustness against various signal processing attacks, and The SSIM is > 9 for majority of the signal processing attacks except JPEG (90% compression) video frames. The robustness for various noise and filtering attacks are above 0.76. The robustness is around 0.6 for JPEG (90% compression). Figure 2(b) shows the robustness against geometrical attacks. For example, Robustness against rotation (45°, 180°), translation (x = 50.3, y = -10.1), circular translation (x = 74, y = 0), rescaling (rescaling to 50% and scaling to 100%), and affine transform (1 1 0:0.33 2 0: 0 1 1). The maximum NCC is about 0.94 and minimum 0.56 for any geometrical attacks. Table 1 shows the pictorial view of the geometrical attacks (shown for the last frame of the test video) and the visual reconstruction of the watermark. It is evident from the Table 1 that the NC values are higher consistently for any kind of geometrical attacks.

In order to have a fair comparison, The suggested plan is contrasted against scheme by Amir et al. [9] and Ranjan et al. [12].

Table 2 demonstrates the robustness analysis. The plan yields superior outcomes for geometrical attacks like rotation, scaling (0.5) and affine transform-vertical and horizontal sheers. The average of attacks are calculated for all three methods to assess the overall robustness. It is shown in Table 2 (last line) that the average robustness is 0.8398 as compared to 0.7335 in Ranjan et al. and 0.5499 in Amir et al. schemes. The PSNR value of the watermarked image is 55.2 dB without attack. This satisfies the imperceptibility of the cover object quality.



(b)

Fig. 2. Experimental results of the proposed scheme (a) image processing attacks (ssim/nc vs. frame no.) (b) geometrical attacks (NCC vs. frame no.)

Table 1. Retrieved watermarks after various geometrical attacks

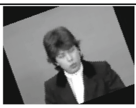
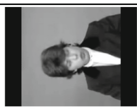
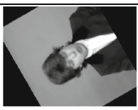
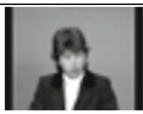
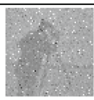
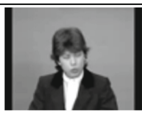
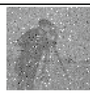
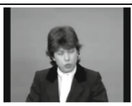
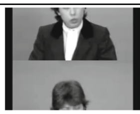
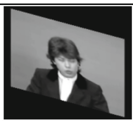
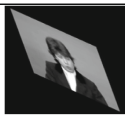
	 0.8324		 0.8691		 0.9184
	 0.8672		 0.6503		 0.7282
	 0.8742		 0.8850		 0.8975
	 0.9083		 0.8509		 0.7800

Table 2. Execution survey of survey of proposed scheme with [9] and [12] based on NCC estimation

Sr. No.	Attacks	Amir et al. [9]	Ranjan et al. [12]	Proposed scheme
1	Rotation (20)	0.0434	0.8265	**0.8324**
2	Rotation (40)	0.0443	0.8736	**0.8791**
3	Rotation (90)	**0.9978**	0.9161	0.9184
4	Rotation (120)	0.0420	0.8613	**0.8692**
5	Scaling (0.25)	0.5789	0.3683	**0.6553**
6	Scaling (0.5)	**0.9864**	0.7022	0.7282
7	Scaling (x2)	**0.9965**	0.9745	0.8742
8	Horizontal Trans [92,0]	0.6911	**0.9991**	0.8850
9	Vertical Trans [0 74] Horizontal +	0.7053	**0.9990**	0.8975
10	Vertical Trans [74 92]	0.4138	**0.9989**	0.9083
11	Vertical sheer	–	0.2113	**0.8509**
12	Horizontal sheer	–	0.0712	**0.7800**
	Average NCC	0.5499	0.7335	**0.8398**

5 Conclusions

The desired strategy is outperforming in robustness and imperceptibility analysis. The average NCC of the proposed scheme is 0.8398 for geometrical attacks. The proposed approach is successfully retrieving the original watermark in the remaining attacks. Also, the quality of the cover object is not being diminished by the proposed strategy because it provides PSNR values greater than 55 dB and picture quality of 0.9 in the majority of signal processing assaults.

References

1. Hsiang- C.H., Chen, Y.H., Lin, G.Y.: DCT-based Robust Watermarking with Swarm Intelligence Concepts. In: 5th Int. conference on Inf. Assurance and Security, Xi'an, China (2009).
2. Sadık Y., Furkan Ü., Hüseyin, S.H.: Digital image watermarking with hybrid structure of DWT, DCT, SVD techniques and the optimization with BFO algorithm. J of polytechnic, 1–1, (2023). doi: https://doi.org/10.2339/politeknik.1192824
3. Moeinaddini, E.: Selecting optimal blocks for image watermarking using entropy and distinct discrete firefly algorithm. Soft computing 23, 9685–9699 (2019).
4. Santhi, V., Manekandan, GRS, Franklin Rajkumar, V.: Entropy based Robust Watermarking Scheme using Hadamard Transformation Technique. IJCA 12(9), 14–21, (2011).
5. Nasrin, M. Makbol, Khoo, B.E., Rassem, T.H.: Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics, IET Image processing 10(1), 34–52, (2016). doi: https://doi.org/10.1049/iet-ipr.2014.0965

6. Xiaobing G. and Xiao B.: Improved Bacterial Foraging Optimization Algorithm with Comprehensive Swarm Learning Strategies. Advances in Swam Intelligence, 12145, 325–334, (2020). doi: https://doi.org/10.1007/978-3-030-53956-6_29
7. Divya J.L., Ranjan K.S.: Feature based robust watermarking using DTT and SVD for copyright protection. IJSST, 19(6), (2018). doi: https://doi.org/10.5013/IJSSST.a.19.06.07
8. Mishra, A., Charu A., Sharma A., Bedi, P.: Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm. ESWA 41(17), 7858–7867, (2014).
9. Amir W., Rajan K.S., Prasad P.M.K.: Robust watermarking in presence of noise. J. of biological research and review, 8(2), 2022. doi: https://doi.org/10.1016/j.eswa.2014.06.011
10. Priya, C., Ramya, C.: Robust and Secure Video Watermarking Based on Cellular Automata and Singular Value Decomposition for Copyright Protection. Circuits, Systems, and Signal Processing, 40, 2464–2493, (2021).
11. Suresh, M., Shatheesh, I.: Optimized interesting region identification for video steganography using Fractional Grey Wolf Optimization along with multi-objective cost function. Journal of King Saud University –CSIS, 34(6), 3489–3496, (2022) doi: https://doi.org/10.1016/j.jksuci.2020.08.007
12. Ranjan K.S., Subodh, S., Prasanth, M.: RST invariant blind image water watermarking scheme using DTT and SVD. AJSE, 45, 3331–3353, (2020). doi: https://doi.org/10.1007/s13369-020-04387-9
13. Nasrin, M., Makbol, Khoo, B.E.: Robust blind image watermarking scheme based on RDWT and SVD.AEUE, 67(2013), 102–112, (2012). doi: https://doi.org/10.1016/j.aeue.2012.06.008