

Firefly optimized robust, imperceptible, secure watermarking scheme

Sushama Subodh Agrawal, Anjali Bhalchandra

Department of Electronics, Government College of Engineering, Aurangabad, India

Article Info

Article history:

Received Apr 13, 2022

Revised Aug 19, 2022

Accepted Aug 30, 2022

Keywords:

Firefly algorithm

Imperceptibility

Lifting wavelet transform

Robustness

Security

Singular value decomposition

ABSTRACT

A multi-objective optimized hybrid image watermarking technique is being proposed considering robustness, imperceptibility and security aspects using two different scaling factors. In this technique, original image is subjected to third level lifting wavelet transform (LWT) followed by singular value decomposition (SVD). Watermark is split into two parts to embed each of them into a different subband. In the suggested scheme, firefly algorithm is employed to get optimum solutions for two scaling factors to balance trade-off amid invisibility and robustness. Security in digitized data is an important aspect of image processing. It is improved with a key, an input to Arnold transform for scrambling watermark, to watermark embedding and extraction procedures. All the performance parameters like peak signal to noise ratio (PSNR), structural similarity index measure (SSIM), normalized correlation coefficient (NCC) and bit error rate (BER) are used in formulating maximization objective function. Evaluation of the proposed algorithm indicates that it is characterized by fairly good robustness, invisibility and security.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Sushama Subodh Agrawal

Department of Electronics, Government College of Engineering

Aurangabad, Maharashtra, India

E-mail: ssa_etx@geca.ac.in

1. INTRODUCTION

The usage of cyberspace and networking technologies for content flow and exchange is rapidly growing. COVID-19, a global pandemic, has greatly increased data transmission. It is essential to avoid modifying these resources without the proper rights or authority. Copyright issues are dealt with using a variety of information security measures. Watermarking digital images [1] is the most effective approach for data authentication and copyright protection [2]. This is accomplished by embedding a text, picture or logo within the original image.

Robustness, imperceptibility and security are important aspects of watermarking techniques. Robustness is the ability of technique to resist attacks on watermarked image whereas imperceptibility indicates the perceptual quality of watermarked image. Embedding approach determines whether the methodology is in spatial or in transform domain. Spatial domain techniques have minimal complexity, easy implementation but are less robust. Transform domain techniques are comparatively more complex as coefficients in transform domain are modified leading to high robustness. The requirement of information during watermark extraction decides whether the process is blind, semi-blind or non-blind. Different transforms like discrete cosine transform (DCT) [3], discrete wavelet transform (DWT) [4], [5], lifting wavelet transform (LWT) [6], stationary wavelet transform (SWT) [7], [8], contourlet transform [9] are used for watermarking solutions. Pros and cons of LWT and DWT based watermarking schemes are discussed

[10]. These transforms are clubbed with matrix decompositions like singular value decomposition (SVD) [11], [12], QR factorization [13]-[15] to achieve enhanced performances. Madhu and Holi [7] discussed a scheme based on SWT, SVD with particle swarm optimization to select optimal coefficients. DWT, DCT and SVD based approach pursued in [11] is more robust to attacks as JPEG compression, Gaussian blur, salt & pepper noise, rotation and cropping with high values of peak signal to noise ratio (PSNR). Similar scheme [16] highlights high robustness against Gaussian attacks. A scheme [12] based on integer wavelet transform, SVD and arnold transform (AT) is used to embed watermarks in a block with lowest variance. The orthogonal U matrix is modified making technique robust against image processing and noising attacks. Touati and Lakhdar [17] presented an efficient scheme based on quantization coefficient and SVD in spatial domain for self-embedding watermarks for compression types of attacks. A watermarking technique using signum of cosine matrix requires less computational time compared to SVD methods, but robustness is good for few attacks [18].

Strength of the watermark embedding depends on scaling factor. Techniques exhibit a trade-off between imperceptibility and robustness with varying scaling factors. A trend is observed in majority of the schemes, that increase in embedding strength helps to improve robustness but has a negative effect on visual transparency. A proper balance is to be achieved by an optimal scaling factor. Nature-inspired algorithms are metaheuristic optimizing methods that imitate the works of nature to solve optimization issues, leading to a new era in computing [19]. Many swarm-based algorithms like firefly algorithm (FA), particle swarm optimization (PSO), artificial bee colony optimization (ABCO), ant colony optimization (ACO) are effectively used for watermarking solutions [20]-[27].

FA is a well-known, effective, competent metaheuristic algorithm used by the researchers to solve the problems in fields of research such as classifications, clustering, neural networks, biomedical engineering, healthcare and other research domains [28]. DWT-SVD based firefly optimized scheme using multiple scaling factor (MSF) [21] offered good imperceptibility and robustness against selected image processing attacks. A scheme based on LWT, FA and regression tree using MSFs [22] contributed good robustness and imperceptibility. A firefly optimized algorithm with DWT and QR decomposition proposed by Guo *et al.* [23] generated comparatively good robustness against some image processing and noising attacks.

Energy compaction and multi-resolution property of LWT helps in designing robust watermarking system [29], [30]. SVD is preferred as slight alteration in singular values do not affect image properties. In this paper, combination of LWT and SVD with FA has been explored for multi-objective optimization using two different scaling factors. A distinct technique is being proposed by splitting scrambled watermark in two different parts and each part is embedded starting from random columns to increase security. A security key 'k' is used as a scrambling parameter to AT and decides column number from where watermark insertion starts.

The following are the paper's main contributions: i) scrambled watermark is divided into two parts and as the size of split watermark is less than subband size, it can be inserted from random column in a subband; ii) secret key 'k' is utilized to scramble watermark as well as it decides the column from where watermark insertion starts in chosen subbands; iii) two different scaling factors are optimized using FA and iv) result validation using a multi-objective function based on PSNR, structural similarity index measure (SSIM), bit error rate (BER) and normalized correlation coefficient (NCC).

This section has included papers employing relevant schemes. Proposed method explaining watermark embedding, extraction and optimization algorithms is described in section 2. Section 3 deals with experimentation results with comparative performance to analyze suggested technique. The conclusions are drawn out in section 4.

2. PROPOSED METHOD

Three level LWT decomposition [31] of the original image gives 32x32 size subbands. LWT helps to remove loss in reconstruction, increases intactness of embedded watermark in the cover image and helps to recover watermark [6], [22]. CH3, CV3 and CD3 are high frequency subbands whereas CA3 is low frequency subband. Choosing the right subband for watermarking is very important. Major image properties are in low frequency subband and watermarking in this subband gives us image with distortions leading to poor imperceptibility. Similarly, diagonal subband is not preferred as it gets eliminated in image operations such as lossy compression. Horizontal and vertical subbands are being used in this scheme with independent scaling factors. Embedding of watermark in singular values of SVD has become increasingly popular as it can resist attacks. Watermarking in LWT-SVD provides good results but an eye is to be kept on security aspect. Different scaling factors are preferred over single scaling factor to achieve better security, invisibility and robustness. A semi-blind scheme combining LWT, SVD and FA is designed to give optimized robustness, imperceptibility and security against false positive detection.

Watermark is scrambled using Arnold transform [32] with secret key ‘k’ an input to embedding and extraction algorithm. Encrypted watermark is divided into two parts of 32x16. SVD is applied to CH3 and CV3 subbands to get orthogonal vectors and diagonal S matrix with size 32x32. Sixteen columns starting from the ‘kth’ column are chosen for watermarking to take care of security aspect.

2.1. Watermark insertion

Original image is 256x256, watermark is 32x32 and security key ‘k’. Procedure for watermarking is as follows: i) original Image *X* is transformed to three level LWT; ii) AT is applied to scramble watermark with key ‘k’ and scrambled watermark *W* is divided into two parts; iii) CH3 and CV3 subbands are chosen for watermarking; iv) SVD is applied to these subbands to get three matrices *U_i, V_i and S_i*; v) singular values *S_i* are altered with scaling factor δ_i and watermark bits starting from kth column to get *S_{1i}*; vi) SVD is applied to *S_{1i}* and it gives watermarked singular values *S_{wi}* and *U_{wi}, V_{wi}*; vii) new watermarked subbands *CH3_w* and *CV3_w* obtained by applying inverse SVD with *S_{wi}, U_i and V_i* and viii) inverse LWT is applied to get watermarked image *X_w*.

2.2. Firefly algorithm

Firefly algorithm was proposed by Yang [33] inspired by flashing behaviour of fireflies. Fireflies communicate with each other using flashlights to attract prey and mates. Following assumptions are made for firefly optimization:

- a) All fireflies are unisexual so each of them can attract other regardless of its sex.
- b) Attractiveness is proportional to brightness. So less bright firefly will move towards brighter one. Brightest firefly flies randomly.
- c) Objective function depicts the brightness of the firefly.

There are two key factors in FA: variation of light intensity and formulating the rate of attraction [22] where attraction rate β is obtained using an analogy with light intensity *I*. For a maximization problem, brightness is proportional to objective function and vice versa for minimization problem.

Light intensity *I_d* is obtained by using inverse square law and absorption coefficient γ as (1).

$$I(d) = I_0 e^{-\gamma d^2} \tag{1}$$

Attraction rate β is defined as (2).

$$\beta = \beta_0 e^{-\gamma d^2} \tag{2}$$

The distance *d_{ij}* among two fireflies *x_i* and *x_j* at *i, j* is given by cartesian distance as (3).

$$d_{ij} = \|x_i - x_j\| = \sqrt{\sum_{k=1}^{dim} (x_{i,k} - x_{j,k})^2} \tag{3}$$

Less bright firefly *x_i* moves towards a brighter one *x_j* using (4):

$$x_i = x_i + \beta_0 e^{-\gamma d_{ij}^2} (x_j - x_i) + \alpha (\text{rand} - \frac{1}{2}) \tag{4}$$

where, *I₀* is original light intensity, β_0 is attractiveness at *d_{ij}* = 0, Second term in (4) is due to attraction and the last term ensures randomness to avoid premature fall into local optimal solution. α is a randomization parameter and term in bracket is random value vector drawn from Gaussian distribution [22].

2.3. Watermark extraction

Watermark is retrieved using key ‘k’, *U_{wi}, V_{wi} and S_{wi}*:

- a) Three level LWT decomposition to watermarked image gives *CA3_{wm}, CD3_{wm}, CH3_{wm}* and *CV3_{wm}* subbands.
- b) SVD is applied to chosen subbands to get singular values *S_{wmi}* required for watermark extraction.
- c) Inverse SVD is applied to *U_{wi}, S_{wmi} and V_{wi}* to get *S_{ei}* matrix.
- d) Watermark bits are obtained from *S_{ei}, S_{wi} and δ_i* and key ‘k’ as clue.

$$W_{ni} = (S_{ei} - S_{wi}) / \delta_i \tag{5}$$

- e) Retrieved bits from two subbands are combined to reconstruct scrambled watermark.

f) Inverse AT is employed for 'k' times to get watermark and performance parameters are computed.

2.4. Parameters for image quality assessment

Assessment of images is very vital to watermarking application as imperceptibility and robustness cannot be decided visually [30], [34], [35]. Metric assessment done mathematically helps to establish and correlate results. Parameters for measuring the performance are defined by:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \quad (6)$$

$$MSE = \frac{\sum_{i=1}^M \sum_{j=1}^N [X(i,j) - X_w(i,j)]^2}{M * N} \quad (7)$$

where X is host, X_w is watermarked image and $M * N$ is size. SSIM index is defined as (8):

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + k_1)(2\sigma_{xy} + k_2)}{(\mu_x^2 + \mu_y^2 + k_1)(\sigma_x^2 + \sigma_y^2 + k_2)} \quad (8)$$

where k_1 and k_2 are two variables used to stabilize division for small denominators, μ_x and μ_y are averages, σ_x , σ_y are standard deviations, σ_{xy} are covariance of x and y images. NCC and BER are computed as (9) and (10):

$$NCC = Corr(w, w') = \frac{\sum_i \sum_j W_{ij} W'_{ij}}{h * w} \quad (9)$$

where w is watermark, w' is extracted watermark,

$$BER = \frac{\text{Mismatched bits}}{\text{Size of watermark}} = \frac{B}{h * w} \quad (10)$$

where h is height and w is width.

2.5. Role of FA in watermark extraction

The performance of the proposed FA is evaluated through maximization multi-objective function to trade-off invisibility and robustness. It is defined using all performance parameters PSNR, SSIM, NCC, BER. BER and NCC are calculated for 29 different attacks.

$$\text{Maximize}(f) = \frac{PSNR}{\omega} + SSIM + \frac{p}{\sum_{k=1}^p BER} + \frac{\sum_{k=1}^p NCC}{p} \quad (11)$$

Where p is number of attacks, ω is the balancing factor.

The different steps for optimization are as follows: i) FA parameters n , α , β_0 , γ , maximum generations are declared; ii) all the 'n' fireflies are initialized randomly in 2-dimensional workspace in the decided range; iii) watermarked image for every firefly is generated by using watermark insertion procedure; iv) PSNR, SSIM are computed between original and watermarked images; v) all the attacks are applied on watermarked image and watermarks are extracted; vi) BER and NCC amid original and extracted watermark are calculated; vii) objective function as given in (11) is evaluated for each firefly; viii) best solution with firefly values is remembered for every iteration; ix) each firefly is updated by computing their new values as per (4); x) fireflies are ranked based on their fitness values (objective function); xi) Steps iii to x are repeated for all the generations and xii) best firefly value in all generations is returned as the best solution i.e. scaling factors in 2-dimensional space.

3. RESULTS AND DISCUSSION

The proposed scheme is evaluated on images downloaded from USC-SIPI database [36]. Gray scale images Lena, Cameraman, Living Room, Mandrill, Peppers and Pirate of size 256x256 are host images and binary watermark is of size 32x32. These standard benchmark images and watermark are shown in Figure 1. Experimental analysis is carried out with parameters initialized as $\beta_0=1$, $\alpha=0.1$, and $\gamma=1$, 12 fireflies and

maximum iterations as 30. Experimentations are performed in Windows 10 based MATLAB (R2020b) environment. Watermarked images with extracted watermarks are shown in Figure 2.

The effectiveness of the proposed scheme is evaluated through parameters PSNR, SSIM, NCC and BER as shown in Table 1. Imperceptibility is perceptual similarity among original and watermarked image indicated by PSNR and SSIM. Watermark is inserted into all chosen images and the optimal scaling factors are computed using FA. Figures 1 and 2 clearly show that it is very difficult to distinguish between them visually. Consistently PSNR values are nearer to 50 and SSIM values are greater than 0.99. Similarly, NCC indicates the similarity and BER shows error bits between original and extracted watermark. NCC is almost near to 0.99 and BER is less than 0.006 for all images indicating fairly good results.

Robustness of the proposed technique against 29 different attacks is depicted in Table 2 for Lena, Pirate and Cameraman images. The suggested system has a bit error rate of around 4% for one or two cropping attacks, but less than 1% for the majority of attacks. The average BER for all attacks is 0.0145, which means the proposed system gives a BER of 1.45%. Attacked images with extracted watermarks for few attacks is shown in Figure 3.



Figure 1. Original images and watermark

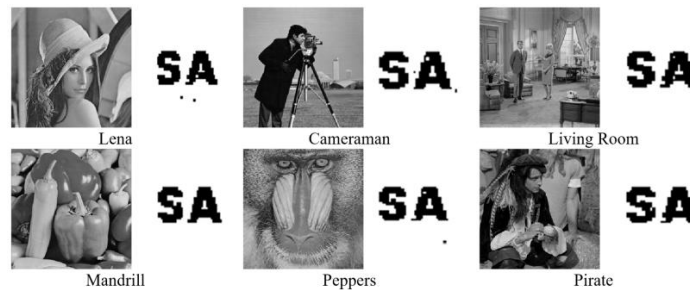


Figure 2. Watermarked images and extracted watermarks for standard images given in Figure 1

Table 1. Results for six benchmark images

Images	Proposed method			
	PSNR	SSIM	NCC	BER
Lena	50.6858	0.9943	0.9831	0.0059
Cameraman	50.9697	0.9746	0.9858	0.0049
Living Room	50.7804	0.9969	0.9915	0.0029
Peppers	50.4411	0.9918	0.9972	0.0009
Mandrill	50.7410	0.9989	0.9887	0.0039
Pirate	50.6860	0.9944	0.9915	0.0029

3.1. Security analysis

Watermarking schemes based on SVD specifically suffer from the problem of false positive detection when watermark is embedded in singular values [37]. This problem is tackled in the current scheme by inserting a security feature using a key which acts as an input to AT, embedding and extraction procedures. Let 'k' be the key to scrambler and insertion procedure, n1 and n2 be the keys to inverse scrambler and to extraction procedure respectively. During watermark insertion, this key is 5. Three different tests conducted are shown:

- a) The decoder has the correct key for inverse scrambler but incorrect key for extraction procedure. Figure 4 shows results for three incorrect inputs.
- b) The decoder has the correct key for extraction procedure but incorrect key to inverse scrambler. Figure 5 shows outputs for different inputs to AT.
- c) The decoder has the incorrect key for extraction procedure and inverse scrambler. Figure 6 shows results for the same.



Figure 3. Attacked watermarked images with extracted watermarks

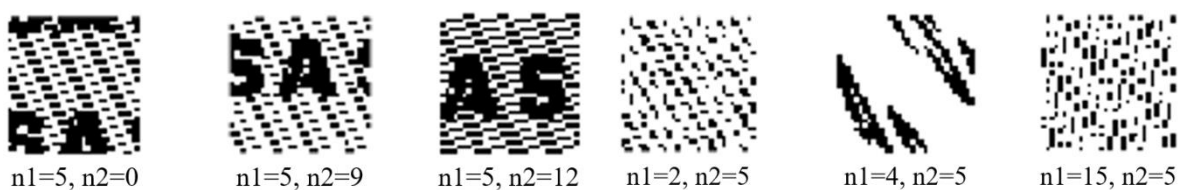


Figure 4. Security test for false keys during extraction

Figure 5. Security test for false keys during inverse AT

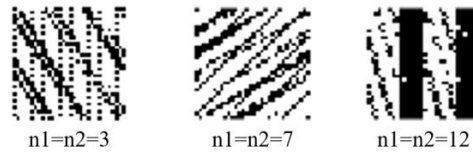


Figure 6. Security test for false key both to inverse AT and extraction procedure

Table 2. Robustness of the proposed technique against various attacks in terms of NCC and BER

Attacks	Parameter	Lena		Pirate		Cameraman	
		NCC	BER	NCC	BER	NCC	BER
Salt & pepper	0.01	0.9689	0.0107	0.9659	0.0117	0.9659	0.0117
	0.02	0.9603	0.0137	0.9520	0.0166	0.9745	0.0088
	0.03	0.9461	0.0186	0.9687	0.0107	0.9319	0.0234
Poisson attack		0.9604	0.0137	0.9607	0.0137	0.9659	0.0117
Speckle noise	0.001	0.9718	0.0098	0.9858	0.0049	0.9858	0.0049
	0.005	0.9801	0.0068	0.9744	0.0088	0.9716	0.0098
	0.009	0.9744	0.0088	0.9773	0.0078	0.9773	0.0078
Gaussian noise	0.001	0.9744	0.0088	0.9689	0.0107	0.9801	0.0068
	0.005	0.9830	0.0059	0.9633	0.0127	0.9716	0.0098
	0.009	0.9630	0.0127	0.9660	0.0117	0.9488	0.0176
Cropping	top left	0.9262	0.0273	0.9098	0.0332	0.9020	0.0352
	centre	0.8837	0.0420	0.9165	0.0313	0.8733	0.0479
	right bottom	0.9213	0.0293	0.9068	0.0342	0.8763	0.0439
Scaling	256→512→256	0.9943	0.0020	0.9943	0.0020	0.9915	0.0029
	128→2561→28	0.9561	0.0156	0.9440	0.0205	0.9558	0.0156
Rotation	90°	0.9112	0.0313	0.9385	0.0215	0.9264	0.0254
	180°	0.9887	0.0039	0.9858	0.0049	0.9915	0.0029
Gamma correction	0.9	0.9752	0.0088	0.9802	0.0068	0.9887	0.0039
	0.6	0.9311	0.0254	0.9773	0.0078	0.9691	0.0107
JPEG	80	0.9943	0.0020	0.9972	0.0010	0.9915	0.0029
	75	0.9887	0.0039	0.9943	0.0020	0.9887	0.0039
	50	0.9801	0.0068	0.9858	0.0049	0.9830	0.0059
Gaussian filter	3x3	0.9801	0.0068	0.9858	0.0049	0.9830	0.0059
	5x5	0.9801	0.0068	0.9858	0.0049	0.9830	0.0059
Low pass filter	3x3	0.9221	0.0283	0.9183	0.0303	0.9291	0.0254
Median filter	3x3	0.9512	0.0176	0.9356	0.0234	0.9376	0.0225
Histogram equalization		0.9745	0.0088	0.9745	0.0088	0.9515	0.0166
Sharpening		0.9744	0.0088	0.9773	0.0078	0.9773	0.0078
Wiener filter		0.9411	0.0215	0.9366	0.0234	0.9461	0.0195

3.2. Comparative analysis

Feature comparison of the proposed technique with a technique in [25] is shown in Table 3. The current scheme is a semi blind watermarking scheme in LWT+SVD domain, embedding with modification of singular values and optimization is implemented using firefly algorithm. Technique discussed in [25] is also a semi blind watermarking scheme in LWT+SVD domain, embedding with modification of singular values and optimization is implemented using artificial bee colony. Imperceptibility and robustness comparison of the proposed technique for image Lena with [25] is represented in Table 4. PSNR values for both the schemes are almost same whereas NCC is slightly higher for [25]. The suggested technique is more robust against most attacks barring few like salt & pepper, cropping and scaling but the parameters for these attacks are not clearly indicated in the reference being used.

Table 3. Feature comparison of proposed scheme with [25]

Features	Proposed	[25]
Scheme type	Semi-blind	Semi-blind
Domain used	LWT+SVD	LWT+SVD
Optimization	Firefly algorithm	Artificial bee colony
Original image size	256x256	512x512
Watermark size	32x32	64x64
Multi-objective	Yes	yes
Fitness function	Function of PSNR, BER, NCC and SSIM	Only NCC
Security analysis	Yes	No

Table 4. Imperceptibility and robustness comparison of proposed technique with [25] for image Lena

Parameters	Proposed	[25]
Imperceptibility		
PSNR	50.6858	50.3469
Robustness (NCC)		
Without attacks	0.9831	1
Salt & pepper	0.9689	0.9832
Poisson	0.9604	0.8757
Speckle noise	0.9718	0.9346
Cropping	0.9262	0.9804
Scaling	0.9943	1
Histogram equalization	0.9745	0.9314
Sharpening	0.9744	0.9194

4. CONCLUSION

The perfect reconstruction and energy compression property of LWT prevents loss in information, aids in the resistance to variety of attacks. Changes in singular values do not alter structural information but only affect luminance of the image thereby making system more robust and imperceptible. The security of the SVD based schemes is enhanced by inserting watermark from random columns. Subbands do contain different information and scaling factor for each of them can be different. Two different optimum scaling factors are computed to decide the watermark embedding strength for maximum performance in each subband. Computation of multiple scaling factors puts a toll on computing speed and this is avoided here by using only two scaling factors. Objective function features all metrics thus helping to improve PSNR, BER, SSIM and NCC in a balanced manner. The main feature of the proposed technique is to apply FA to find optimum scaling factors for balancing the trade-off giving PSNR, NCC and SSIM greater than 50 dB, 0.96, 0.9940 respectively and average BER less than 1.45%. Comparative analysis indicates that the proposed technique gives almost same imperceptibility but robustness has improved to a great extent. Security analysis is also an added feature in the current scheme while doing comparative analysis. It can be said current scheme is highly robust, imperceptible and secure against non-authorized access of the content and it can be practically used for any applications wherein copyright violations are to be avoided.




REFERENCES

- [1] F. Ernawan, "Robust image watermarking based on psychovisual threshold," *Journal of ICT Research and Applications*, vol. 10, no. 3, pp. 228–242, 2016, doi: 10.5614/itbj.ict.res.appl.2016.10.3.3.
- [2] F. Qasim, A. Al-Yousuf, and R. Din, "Review on secured data capabilities of cryptography, steganography, and watermarking domain," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 17, no. 2, pp. 1053–1059, 2020, doi: 10.11591/ijeecs.v17.i2.pp1053-1059.
- [3] S. N. Prajwalasimha, S. S. Chethan, and C. S. Mohan, "Performance analysis of DCT and successive division based digital image watermarking scheme," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 15, no. 2, pp. 750–757, Aug. 2019, doi: 10.11591/ijeecs.v15.i2.pp750-757.
- [4] E. Najafi, "A robust embedding and blind extraction of image watermarking based on discrete wavelet transform," *Mathematical Sciences*, vol. 11, no. 4, pp. 307–318, Dec. 2017, doi: 10.1007/s40096-017-0233-1.
- [5] L. Lidyawati, A. R. Darlis, L. Jambola, L. Kristiana, and R. R. Jayandanu, "Digital watermarking image using three-level discrete wavelet transform under attacking noise," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 11, no. 1, pp. 231–238, Feb. 2022, doi: 10.11591/eei.v11i1.3565.
- [6] V. S. Verma and R. K. Jha, "Improved watermarking technique based on significant difference of lifting wavelet coefficients," *Signal Image Video Process*, vol. 9, no. 6, pp. 1443–1450, Sep. 2015, doi: 10.1007/s11760-013-0603-6.
- [7] B. Madhu and G. Holi, "An optimal and secure watermarking system using SWT-SVD and PSO," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 18, no. 2, pp. 917–926, May 2020, doi: 10.11591/IJECS.V18.I2.PP917-926.
- [8] R. A. El-Shahed, M. N. Al-Berry, H. M. Ebied, and H. A. Shedeed, "High capacity video hiding based on multi-resolution stationary wavelet transform and hybrid-matrix decomposition techniques and hybrid-matrix decomposition techniques," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 11, no. 4, pp. 1959–1969, Aug. 2022, doi: 10.11591/eei.v11i4.2922.
- [9] J. N. Shehab, H. A. Abdulkadhim, and Y. Allbadi, "Blind image watermarking scheme based on lowest energy contourlet transform coefficient and modified arnold cat/ikeda maps," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 21, no. 1, pp. 196–207, Jan. 2021, doi: 10.11591/ijeecs.v21.i1.pp196-207.
- [10] D. B. Taha, T. B. Taha, and N. B. Dabagh, "A comparison between the performance of DWT and LWT in image watermarking," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 9, no. 3, pp. 1005–1014, Jun. 2020, doi: 10.11591/eei.v9i3.1754.
- [11] M. Awasthi and H. Lodhi, "Robust image watermarking based on discrete wavelet transform, discrete cosine transform and singular value decomposition," *Journal of Electronic Imaging*, vol. 21, no. 3, pp. 033005-1–033005-7, 2012, doi: 10.1117/1.JEI.21.3.033005.
- [12] F. Ernawan and D. Ariatmanto, "Image watermarking based on integer wavelet transform-singular value decomposition with variance pixels," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 3, pp. 2185–2195, Jun. 2019, doi: 10.11591/ijece.v9i3.pp2185-2195.
- [13] W. Song, J.-J. Hou, Z.-H. Li, and H. Liang, "Chaotic system and QR factorization based robust digital image watermarking algorithm," *Journal of Central South University of Technology*, vol. 18, 2011, doi: 10.1007/s11771-011-0668-8.
- [14] A. M. Abduldaim and M. Q. Hamid, "Robust image watermarking based on QR factorization and LWT," *International Journal of Engineering & Technology*, vol. 7, no. 4, pp. 5358–5362, 2018, doi: 10.14419/ijet.v7i4.23661.
- [15] A. Sushama and B. Anjali, "Robust imperceptible gray image watermarking with LWT SVD and QR decomposition," *International Journal of Computer Theory and Engineering*, vol. 14, no. 3, pp. 89–96, 2022, doi: 10.7763/IJCTE.2022.V14.1315.
- [16] M. N. Abdulwahed and A. K. Ahmed, "Improved anti-noise attack ability of image encryption algorithm using de-noising technique," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 6, pp. 3080–3087, Dec. 2020, doi: 10.12928/TELKOMNIKA.v18i6.16384.
- [17] N. E. Touati and A. M. Lakhdar, "Self embedding digital watermark using hybrid method against compression attack," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 24, no. 2, pp. 864–870, Nov. 2021, doi: 10.11591/ijeecs.v24.i2.pp864-870.
- [18] F. Ernawan, P. W. Adi, S. C. Liew, E. A. Sarwoko, and E. Winarno, "Fast image watermarking based on signum of cosine matrix," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 25, no. 3, pp. 1383–1391, Mar. 2022, doi: 10.11591/ijeecs.v25.i3.pp1383-1391.




- [19] N. Dey, J. Chaki, L. Moraru, S. Fong, and X.-S. Yang, "Firefly algorithm and its variants in digital image processing: a comprehensive review," in *Applications of Firefly Algorithm and its Variants: Case Studies and New Developments*, N. Dey, Ed. Singapore: Springer Singapore, 2020, pp. 1–28. doi: 10.1007/978-981-15-0306-1_1.
- [20] K. Loukhaoukha, M. Nabti, and K. Zebbiche, "A robust SVD-based image watermarking using a multi-objective particle swarm optimization," *Opto-Electronics Review*, vol. 22, no. 1, pp. 45–54, 2014, doi: 10.2478/s11772-014-0177-z.
- [21] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm," *Expert Systems with Applications*, vol. 41, no. 17, pp. 7858–7867, Dec. 2014, doi: 10.1016/j.eswa.2014.06.011.
- [22] B. Kazemivash and M. E. Moghaddam, "A robust digital image watermarking technique using lifting wavelet transform and firefly algorithm," *Multimed Tools Applications*, vol. 76, no. 20, pp. 20499–20524, Oct. 2017, doi: 10.1007/s11042-016-3962-5.
- [23] Y. Guo, B. Z. Li, and N. Goel, "Optimised blind image watermarking method based on firefly algorithm in DWT-QR transform domain," *IET Image Process*, vol. 11, no. 6, pp. 406–415, Jun. 2017, doi: 10.1049/iet-ipr.2016.0515.
- [24] I. A. Ansari, M. Pant, and C. W. Ahn, "Artificial bee colony optimized robust-reversible image watermarking," *Multimed Tools Applications*, vol. 76, no. 17, pp. 18001–18025, 2017, doi: 10.1007/s11042-016-3680-z.
- [25] A. M. Abdulazeez, D. M. Hajy, D. Q. Zeebaree, and D. A. Zebari, "Robust watermarking scheme based LWT and SVD using artificial bee colony optimization," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 21, no. 2, pp. 1218–1229, Feb. 2020, doi: 10.11591/ijeecs.v21.i2.pp1218-1229.
- [26] S. Khan and T. Bianchi, "Ant colony optimization (ACO) based data hiding in image complex region," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 1, pp. 379–389, Feb. 2018, doi: 10.11591/ijece.v8i1.pp379-389.
- [27] T. Salehnia and A. Fathi, "Fault tolerance in LWT-SVD based image watermarking systems using three module redundancy technique," *Expert Systems with Applications*, vol. 179, Oct. 2021, doi: 10.1016/j.eswa.2021.115058.
- [28] J. Nayak, B. Naik, P. Dinesh, K. Vakula, and P. B. Dash, "Firefly algorithm in biomedical and health care: Advances, issues and challenges," *SN Computer Science*, vol. 1, no. 6, p. 311, 2020, doi: 10.1007/s42979-020-00320-x.
- [29] V. S. Verma, R. K. Jha, and A. Ojha, "Significant region based robust watermarking scheme in lifting wavelet transform domain," *Expert Systems with Applications*, vol. 42, no. 21, pp. 8184–8197, Jul. 2015, doi: 10.1016/j.eswa.2015.06.041.
- [30] M. Islam and R. H. Laskar, "Geometric distortion correction based robust watermarking scheme in LWT-SVD domain with digital watermark extraction using SVM," *Multimedia Tools and Applications*, vol. 77, no. 11, pp. 14407–14434, 2018, doi: 10.1007/s11042-017-5035-9.
- [31] W. Sweldens, "The lifting scheme: A construction of second generation wavelets," *SIAM Journal on Mathematical Analysis*, vol. 29, no. 2, pp. 511–546, 1998, doi: 10.1137/S0036141095289051.
- [32] N. Saikrishna and M. G. Resmipriya, "An invisible logo watermarking using arnold transform," in *Procedia Computer Science*, 2016, vol. 93, pp. 808–815, doi: 10.1016/j.procs.2016.07.299.
- [33] X.-S. Yang, "Firefly algorithms for multimodal optimization," in *SAGA 2009: Stochastic Algorithms: Foundations and Applications*, 2009, pp. 169–178, doi: 10.1007/978-3-642-04944-6_14.
- [34] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004, doi: 10.1109/TIP.2003.819861.
- [35] M. Islam, A. Roy, and R. H. Laskar, "SVM-based robust image watermarking technique in LWT domain using different sub-bands," *Neural Computing and Applications*, vol. 32, no. 5, pp. 1379–1403, 2020, doi: 10.1007/s00521-018-3647-2.
- [36] A. G. Weber, "The USC-SIPI image database," SIPI-USC ,2006, [Online], <http://sipi.usc.edu/services/database/Database.html>."
- [37] J.-M. Guo and H. Prasetyo, "False-positive-free SVD-based image watermarking," *Journal of Visual Communication and Image Representation*, vol. 25, no. 5, pp. 1149–1163, 2014, doi: <https://doi.org/10.1016/j.jvcir.2014.03.012>.

BIOGRAPHIES OF AUTHORS



Sushama Subodh Agrawal    received B.E. degree in Electronics from Bombay University in 1988 and M.E. Degree in Electronics from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, India in 2001. She is presently working for Ph.D. degree in electronics engineering at Dr. Babasaheb Ambedkar Marathwada University, Aurangabad. Her research interests include image processing, embedded systems and VLSI. She has 28 plus years of teaching experience at Diploma, UG and PG levels. She has presented and published nearly 20 technical papers at National and International level. Mrs. S.S. Agrawal is life member of Indian Society for Technical Education (ISTE) India. She can be contacted at email: ssa_etx@geca.ac.in.



Anjali Bhalchandra    received B.E. Electronics and Telecommunication degree in 1985 from Gulbarga University, Karnataka and M.E. Electronics degree in 1992 from Marathwada University, Aurangabad. She completed her Ph.D. in electronics engineering from S.R.T.M. University, Nanded, India, in 2004. She has a scientific and technical background covering wide areas of electronics and communication. Currently, she is Principal, Government College of Engineering, Aurangabad and Professor, Electronics Department. Her research interests include image, signal processing and communication. She has 33 plus years of teaching experience at UG and PG levels. She has published more than 100 technical papers in various reputed journals and conference proceedings. Dr. Bhalchandra is a fellow of the Institution of Engineers (IE), India and life member of Indian Society for Technical Education (ISTE) India. She can be contacted at email: asbhalchandra@gmail.com.