

A Digital Image watermarking system for Securing Multimodal biometric modalities using Whale Optimization Algorithm.

* R Devi¹, K Sharmila², C Shanthi³, J Jebathangam⁴

¹ Asst. Prof. Dept. Of Computer Science, VISTAS,

² Associate Prof. Dept. of Computer Science, VISTAS ,

³ Asst. Prof. Dept. of Computer Science, VISTAS ,

⁴ Asst. Prof. Dept of Computer Science, VISTAS ,

Abstract. Authentication and identification has become a big challenge in this fast growing world. The traditional method of identifying an individual includes PIN number, user name, password etc., and those techniques are easily duplicated, misused or shared. To avoid the above pitfalls, biometric comes into existence. Biometric system is an automatic identification of an individual using their physiological or behavioral traits. These biometric traits are stored in the database digitally. Nowadays, since data breach has become quite common, leakage of these biometric traits has a direct impact on the individual. Hence, the biometric traits are secured using one of the information hiding techniques named digital watermarking. Robustness and imperceptibility are the two predominant factors of watermarking system. In this article, multimodal biometric traits such as fingerprint and iris are fused using Gradient Pyramid algorithm (GP). This fused biometric template acts as watermark. The watermark is then embedded into the cover image, Lena of size 256X256. Whale optimization algorithm (WOA) is used to find the optimum position to embed the watermark in order to improve the robustness of the watermark. Performance of WOA is measured using the performance measures such as Peak-Signal-Noise-Ratio (PSNR), Normalized cross correlation (NCC) and Structural Similarity Index (SSIM). The algorithm is more robust when compared with other existing algorithms with a PSNR of 90.3420 SSIM as 1 and NC as 1.

Keywords: *Biometric, Watermarking, WOA, PSNR, NC, SSIM*

1. INTRODUCTION

Digital watermarking is a standard technology used for broadcast monitoring, security and authentication of digital media [1]. Digital watermarking is a technique used to implant information into digital data which cannot be easily identified by unauthorized users. The techniques have been used in biometric system in order to secure and authenticate biometric data and also to increase the level of accuracy for recognition. [2] A Biometric System is an automatic identification of an individual. The digital form of the biometric characteristics is known as a biometric template. As per the recent senses, iris and fingerprint authentication growth rate is high when compared to others. Biometric system faces some major problems when the system depends on a single biometric feature. For example, now and then our voice is subject to change due to severe cold or throat infection and also the quality of the fingerprints may be lost or diminished due to several reasons such as dirty finger, injury in the finger, dirty sensor surface and also because of the disposition of the finger on the sensor. So to conquer the above limits of the uni-modal

biometric system, multi-modal comes into existence.. The system merges two or more biometric templates such as fingerprint and iris, face and fingerprint, etc.,.

2. RELATED WORK

[3] have proposed a new novel optimization method named “Grey Wolf Optimizer (GWO)” for digital images in wavelet transform. Positioning the watermark in a cover image plays a major role. GWO Technique is used to find the optimum value.. The technique was analyzed using “Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE).[3], have summarized the importance of digital watermarking techniques and also discussed about the two major optimization techniques namely “Particle Swarm Optimization (PSO) and Genetic Algorithm (GA)”Discrete Wavelet Transform was used by the two optimization techniques and manipulated that PSO algorithm got “PSNR as 53 and MSE as 0.0039” whereas GA got the “PSNR AS 50.5 and MSE AS 0.0048”.From the experimental results, PSO on 100 iterations provides a better result than GA, “ [4],GA is used to find the feasible value using the fitness function to be formulated. The Gaussian science was also used to find the efficiency of the technique.[5], demonstrated a “Multi-objective evolutionary optimizer (MEO)” based on highly protected and strongly unique image watermarking technique using DWT and SVD. In this scheme, the watermark is scrambled using Fibanocci series.[6], have narrated a hybrid watermarking system with an image fusion technique. The author used multimodal biometric system and fused the traits using three fusion algorithms namely “PCA, DWT, Laplacian Pyramid and HIS.” In this work BFOA algorithm was proposed for watermark embedding. The technique was implemented in MATLAB 7.14.[7] , described a new algorithm namely “Multi-objectives Bees algorithm (MOBA)”. MOBA technique was performed to calculate the best co-efficient using DCT.(Nair et al., 2014), proposed a novel technique that works on three biometric modalities namely Palmprint , Fingerprint & iris and are fused with min or max technique. The author uses PSO algorithm to manipulate the scaling factor in order to find the optimum value.[8] , discussed the major factor in watermarking system that choosing a optimum position was the promising factor. In this defined work, the author decomposes the cover image into four sub-bands. Once again decompose the sub-band LL into 4x4 blocks. Apply SVD to every block in LL. The most reliable technique named singular value decomposition was used with Particle Swarm Optimization (PSO) to find the best scaling factor. [9], have developed a technique using “Differential Evolution (DE)” algorithm fused with “SVD & DWT. The DE algorithm was used to. The watermark was further scrambled using “Arnold Transform” to improvise the security. The experimental discussion concludes that the proposed work gives a satisfactory result that retains the quality of the cover image as well the watermark sustainability.

3. METHODOLOGY

The proposed Watermarking consists of five phases. It includes Image Acquisition, Pre-Processing and Segmentation, Fusion of Images, Encryption and Embedding Extracting procedure. The below Figure 1 illustrates the Schematic diagram of the proposed methodology. The two biometric modalities namely fingerprints and iris acquired from the existing dataset FVC2000 and UBIRIS.VI. The acquired images were pre-processed using Wiener filter and the iris was segmented using Daughman;s rubber sheet model. Then the biometric templates are fused using three fusion techniques namely DWT, Gradient Pyramid and PCA. In this paper, fingerprint and iris are fused using a technique called gradient pyramid. The fused Template is further encrypted using Honey Encryption for higher level security. The encrypted fused template acts as a watermark. A hybrid approach namely DWTSVDWOA has been proposed to find the optimum position

for watermark embedding into the original (i.e) cover image that undergoes some transformation. The experimental investigations are carried out to maintain the robustness and the imperceptibility of the watermarked system. The proposed system is compared with other existing techniques. Fig.1 shows the proposed model.

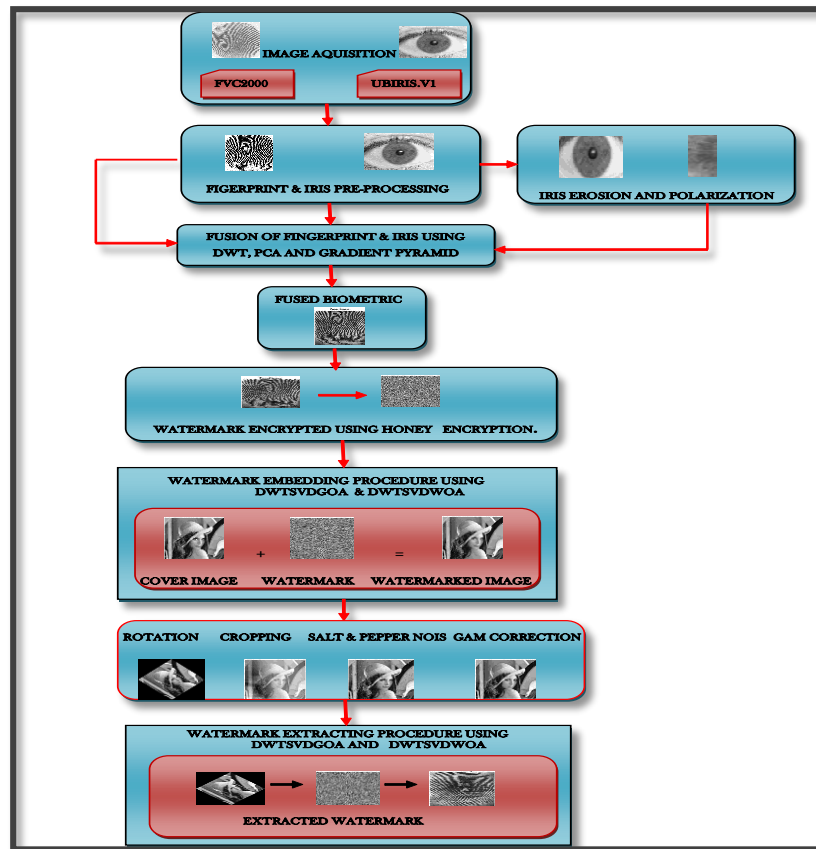


Figure 1 . Proposed Watermarking System

[2]One of the critical and challenging tasks in the watermarking system is to determine the scaling factor. In the conventional methods the scaling factor is determined by choosing a random position .Among the random positions which position sustains the image quality to a maximum level (i.e) which position yields a higher PSNR value will be selected as a scaling factor for embedding.

In the system; the scaling factor determines the potentiality of the watermark which determines the Robustness and the imperceptibility of the scheme.[2] If the scaling factor is too small, the watermark will not be visualized appropriately and less robust to common attacks. If the scaling factor is high, the quality of the watermarked image is degraded. Therefore, the selection of an optimal scaling factor to embed the watermark enables the digital watermarking system as an optimization problem. So, a hybrid watermarking technique (DWTSVDWOA) using was proposed. The below Fig 2 & 3 shows the Input Fingerprint images and eyes .Fig 4 & 5 shows the enhanced and segmented fingerprint & iris and the Fig 6(a) & (b) gives the fused biometric template and encrypted template using honey encryption.

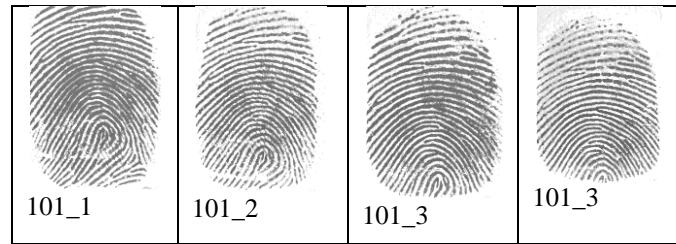


Figure 2. Input Fingerprint images

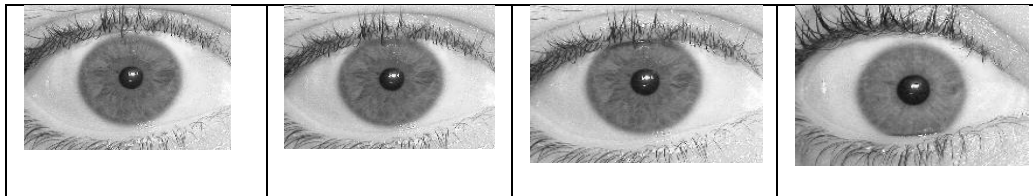


Figure 3. Input eyes images



Figure 4. Pre-Processed Fingerprint Images

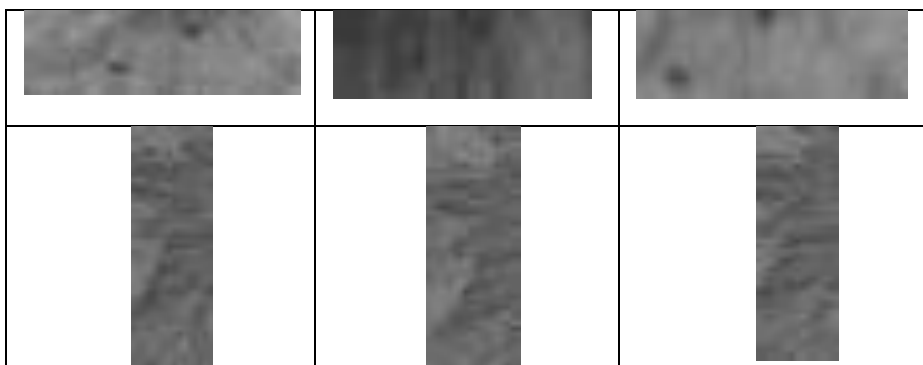


Figure 5. Segmented Iris Images

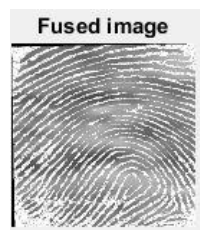


Figure 6(a). Fused Template using GP

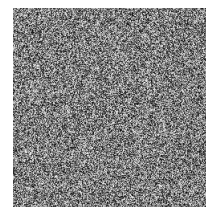


Figure. 6(b) Encrypted Fused Template

3.1 Proposed Algorithm -DWTSVDGOA

The proposed Algorithm DWTSVDWOA fuses the two existing techniques DWT and SVD for decomposition and transformation in order to embed the watermark (encrypted fused multimodal biometric traits) in an optimum scaling factor. [10] The population is initiated using a Whale optimization technique (WOA) to find the best possible position to implant the watermark. This WOA algorithm is fused with the existing techniques namely DWT and SVD to strengthen the watermarking model. The Whale optimization algorithm is used to find the optimal scaling factor for watermarking to achieve the robustness and the imperceptibility of the scheme. The watermark is invisible to the human eyes. So, it is more essential to examine the reliability of the watermarked image. Robustness defines the strength of the watermark.. The eminence of the extracted watermark is measured by analyzing the performance metrics. [10].
The fitness function is given by combining the three metrics is stated in the below equation 1. [2].

$$\text{Fitness } F = \frac{PSNR}{100} \times \text{Max}[\sum_{i=1}^n NC(w, w')] \times SSIM(w, w') \quad (1)$$

Table 1. Pseudo code for Watermark Embedding & Extracting Algorithm (DWTSVDWOA)



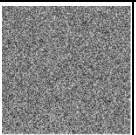



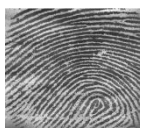
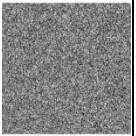




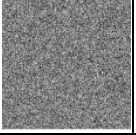




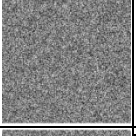



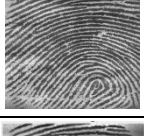
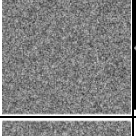

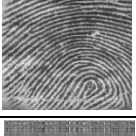

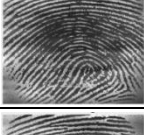
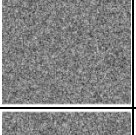

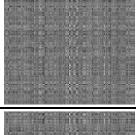


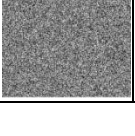

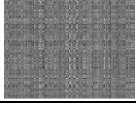
Watermark embedding Algorithm DWTSVDWOA	Watermark embedding Algorithm DWTSVDWOA
<p>STEP 1: Decompose the grey-level cover image into single-level Decomposition using Haar Wavelet $[LL, LH, HL, HH] = \text{Dwt}(\text{Cover_image})$</p> <p>STEP 2: Apply SVD to LL band of the Cover image found in STEP 2 $[U_imgr1, S_imgr1, V_imgr1] = \text{SVD}(LL)$</p> <p>STEP3: Initialize the Whales, iteration, lower bound, upper bound and the objective Function.</p> <p>STEP 4: Check the boundaries of the search space, cover image found in STEP 2.</p> <p>STEP 5: Calculate and identify the fitness function for all the population. $\text{Fitness } F = \frac{PSNR}{100} \times \text{Max}[\sum_{i=1}^n NC(w, w')] \times SSIM(w, w')$</p> <p>STEP 6: Best fitness function is selected to find the optimum scaling factor using WOA.</p> <p>STEP 7: Read the encrypted fused biometric template as a watermark of size MXN using Honey Encryption</p> <p>STEP 8: Apply single-level Dwt to the Watermark (encrypted watermark) $[LL, LH, HL, HH] = \text{Dwt}(\text{Watermark_image})$</p> <p>STEP 9: Apply SVD to LL band of the Watermark image found in STEP 8 $[U_imgr2, S_imgr2, V_imgr2] = \text{SVD}(LL)$</p> <p>STEP 10: Embed the modified watermark image found in step 12, into the optimum position and is manipulated through the fitness function found in STEP 6.</p> <p>STEP 11: Apply inverse SVD to LL subband.</p> <p>STEP 12: Apply Single level inverse dwt get the Watermarked image. $\text{Watermarked image} = \text{idwt}(\text{New LL, New LH, New HL, New HH})$</p> <p>STEP 13: Display the Cove Image, Watermarked image</p>	<p>STEP 1: Read the Watermarked Image of size MXN.</p> <p>STEP 2: Apply all the possible geometric attacks and signal operations to the watermarked image to analyze the robustness of the proposed method.</p> <p>STEP 3 : Extract and Decrypt the Watermark</p> <p>STEP 4 : Apply idwt to the watermark $\text{Recovered } [LL, LH, HL, HH] = \text{IDWT}(\text{Watermark})$</p> <p>STEP 3: Apply inverse SVD to LL sub-band of the watermark found in STEP 4. $[U, S, V] = \text{ISVD}(LL)$</p> <p>STEP 5: Calculate the PSNR, NC and SSIM for the watermark.</p> <p>STEP 6: When SSIM & NC is equals to 1, the algorithm sustain the quality of watermark before and after embedding</p>

The above table 1 shows the algorithm for watermark embedding and extracting.

4. RESULTS AND DISCUSSION

[2]In this work, the Robustness of the proposed method, DWTSVDWOA is analyzed by the simulation results. All simulation results are carried out on a personal computer having Intel Core i3 CPU @, 1.90 GHz with 4.00 GB RAM and using MATLAB Version R2015a under Windows 7 environment. Three-Benchmark images Lena, Cameraman, and Boat of size 256x256 have been used as a cover image [2]. A fused encrypted multimodal biometric has been used as a watermark of size 256x256. The performance of the proposed algorithm DWTSVDWOA is depicted in the below tables.


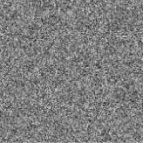


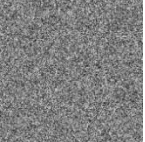


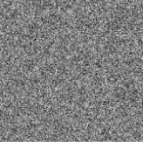


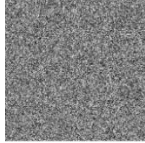


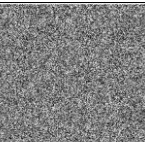




Table 2. Robustness of Watermarked image using DWTSVDWOA under various Signal Processing and geometric attacks for the cover image Lena

S.no	Attack Type	Cover Image	Fused biometric image(water mark)	Encrypted Watermark	Watermarked image with Attack	Extracted watermark	PSNR	NCC	SSIM
1	Gamma Correction						58.2910	0.9551	1
2	Cropping						60.9737	0.9734	0.9986
3	Salt & Pepper Noise						60.6525	0.9719	1
4	Gaussian Attack						72.2113	0.9845	1
5	Rotation						59.3074	0.9657	0.9898
6	Jpeg Attack						58.6748	1.4	1
7	Scaling						58.0956	1.4	1

The above table 2 provides the robustness of the Proposed method (DWTSVDWOA). The table consists of the Cover Image Lena (256x256), fused multimodal template, Encrypted fused template (Watermark Image) of size 256x256. To investigate the robustness of the DWTSVDWOA, the watermarked image undergoes some geometric attack and signal processing operations such as Gamma correction, Cropping, scaling, Rotation, salt & pepper noise, Gaussian attack and so on. From

the transformed watermarked image, the watermark is extracted. The quality of the extracted watermark is ascertained using the metrics PSNR, NC, and SSIM. The extracted watermark after Gaussian attack is 75.2113 whereas for other attacks it may vary from 58 to 60

Table 3. Imperceptibility of DWTSVDWOA for the cover images

Cover Image (256x256)	Watermark (256x256)	Watermarked Image	PSNR	SSIM	NC
			88.1441	0.9267	0.9257
			89.3420	1	1
			88.5436	0.9876	0.9679
			89.5549	1	1
			89.2667	1	1
			87.6239	0.8978	0.8761

In the table 3, the imperceptibility of the proposed method DWTSVDWOA is analyzed using the metrics PSNR, NC, and SSIM.

5. PERFORMANCE OF DWTSVDWOA WITH EXISTING TECHNIQUES

Table 4 .Comparing the PSNR & NC values of DWTSVDWOA with the existing methods to ensure Imperceptibility for Lena image

S.NO	EXISTING TECHNIQUES	PSNR	NC	REFERENCES
1	DWTSVDWOA	90.3420	1	Proposed Algorithm
3	Flirefly +DWT-QR	71.4520	0.98	Yong Guo et al.,2017
4	GA + DWT	52.5632	0.88	Ramanjaneyulu & Rajarajeswari 2012
5	Bacterial Foraging Optimization Algorithm(BFOA)	55.5	0.96	S.Anu H.Nair, et al.,2015
6	Hybrid DWT-SVD	79.8611	1	Baisa L.Gunjal ^{1*} and Suresh N.Mali ² , 2015
7	SVD – Firefly	63.786	1	K. Vijaya Durga et al.,2015
8	DWT-GWO	61.1463	0.88	Priyanka Panwar et al.,2017

The Imperceptibility of DWTSVDWOA with other existing techniques in terms of PSNR & NC is also shown in the below Figure 7(a) & (b)

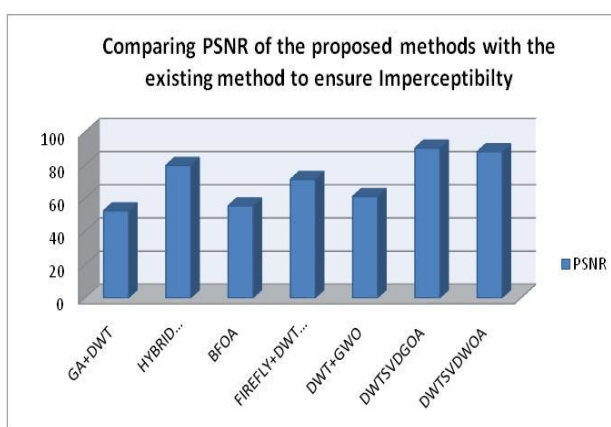


Figure 7(a) PSNR

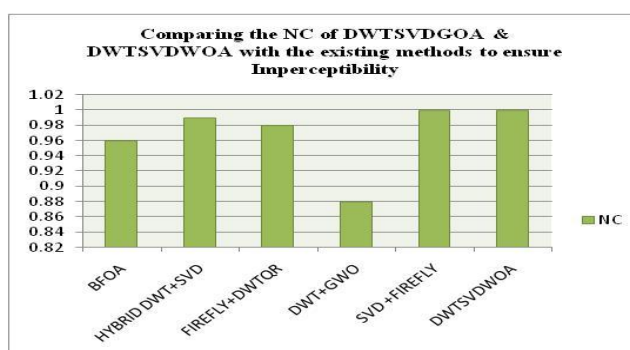


Figure 7(b) NC

Table 5. Comparing the Robutness of DWTSVDWOA Methods with the Existing Methods in terms of NC , SSIM

EXISTING METHODS	ATTACK TYPES									REFERENCES
	Gamma Correction(0.9)	Rotation	Salt & Pepper Noise	Cropping Attack	Gaussian Noise(0.01)	Histogram	Scaling	Median Filter(3x3)	Compression	
DWTSVDWOA	1	1	1	0.9986	1	1	0.9989	1	1	Proposed
GA+DWT	0.9983	0.5695	0.9263	-	0.3922	0.888		0.813	0.9375	Ramanjaneyulu et al.,
DWT+SVD	0.99		0.93	-	0.8	0.99		0.96	0.816	Azizi et al.,
FIREFLY-DWTQR	0.942	0.9629		-	0.9245		0.9336		0.9314	Yong Guo, et
MEO BASED DWT+SVD	0.9997	0.9951	0.9817	0.9872	0.9817	0.9951		0.9972	0.9789	Baisa L Gunjal1 et al
FIREFLY SVD	-	-	-	0.56	0.78	-	0.9	-	1.62	K. Vijaya Durga et al.,

The above table 5 gives a quality of the extracted watermark after making possible attacks on the watermarked image. The analysis is measured using the metric SSIM. It was very clear that the proposed method(**DWTSVDWOA**) retain the similarity of the watermark before and after embedded even after the simulated attack

Table 6. Comparing the Robutness of DWTSVDWOA Methods with the Existing Methods in terms of PSNR

EXISTING TECHNIQUES	ATTACK TYPES									REFERENCES
	Gamma Correction(0.9)	Rotation	Salt & Pepper Noise	Cropping	Gaussian Noise (Density 0.001	Histogram	Scaling	Median Filter(3x2)	Compression (Q.F.60%)	
DWTSVDWOA	58.291	60.9737	60.6525	60.9737	72.2113	59.3074	58.0956	56.8723	58.6748	PROPOSED
PSO	-	-	28.13	-	-	-	-	35.56	38.72	Punam Bedi et al
DWT+SVD	20.1435	11.4089	12.3335	13.0455	29.863	17.5452	29.7727	32.8472	8.3348	Jane O et al
DWT+SVD+DE	25.1796	22.3078	-	18.4203	-	23.0245	-	-	-	Mr.K.Balasamy et al.,2016
PSO+SVD	22.7497	10.163	24.2177	15.175	34.4528	16.6719	33.2454	34.3906	26.8778	Falgun Thakkar, et al
CUKCOO SEARCH	-	-	11.1779	24.774	13.9981	-	15.9314	-	-	Bhargavi Latha et al

The above table 6 gives an image quality of the extracted watermark after making possible attacks The analysis is measured using the metric PSNR. It was very clear that the proposed method (**DWTSVDWOA**) resist and protect the watermark embedded even after the simulated attack

6. CONCLUSION

A hybrid image watermarking system was developed and implemented successfully. The performances of the proposed method DWTSVDWOA was evaluated using the metrics PSNR, SSIM, and NCC. The performance analysis was carried out with existing methods, and the result shows that the DWTSVDWOA provides good robustness and imperceptibility. It also shows that the proposed method (DWTSVDWOA) gives good robustness for cropping with the scaling factor of about 0.001.The proposed

techniques achieved normalized correlation as 1 for all cover images indicating that the exact recovery of the watermark with NC is 1 and also DWTSVDWOA method produces PSNR 90.3420 for the Lena, 89.1121 for the cameraman and the boat 89.5436.

References

- [1] Devi, R., & Sujatha, P. (2015). An Overview of Digital Watermarking with a Performance Analysis of Wavelet Families for Image Compression. *Indian Journal of Science and Technology*, 8(29), 1–5. <https://doi.org/10.17485/ijst/2015/v8i29/85286>
- [2] Devi R., Sujatha P. (2020) A Hybrid Watermarking System for Securing Multi-modal Biometric Using Honey Encryption and Grasshopper Optimization Technique. In *Intelligent Computing and Innovation on Data Science. Lecture Notes in Networks and Systems*, vol 118. Springer, Singapore. https://doi.org/10.1007/978-981-15-3284-9_83.
- [3] Panwar, P., & Sharma, R. (2017). Robust Digital Image Watermarking based on Hybrid DWT and GWO Optimization Technique, 7(10), 9790. <https://doi.org/10.9790/9622-0710041217>
- [4] Al-allaf, O. N. A. (2017). Particle Swarm Optimization Algorithm vs . Genetic Algorithm for Image Watermarking Based Discrete Wavelet Transform, 11(9), 1106–1112.
- [5] Gunjal, B. L. (2015). MEO based secured , robust , high capacity and perceptual quality image watermarking in DWT- SVD domain. <https://doi.org/10.1186/s40064-015-0904-z>
- [6] Nair, S. A. H., & Aruna, P. (2015). Comparison of DCT , SVD and BFOA based multimodal biometric watermarking systems. *Alexandria Engineering Journal*, 54(4), 1161–1174. <https://doi.org/10.1016/j.aej.2015.07.002>
- [7] Lee, J., Wang, J., & Giang, K. (2014). A New Image Watermarking Scheme using Multi- Objective Bees Algorithm, 2953(6).
- [8] Thakkar, F., & Srivastava, V. K. (2017). A particle swarm optimization and block-SVD-based watermarking for digital, 3273–3288. <https://doi.org/10.3906/elk-1603-17>.
- [9] Balasamy, K., Priyanka, S., Kavya, N., Shruthi, A. A., Balasamy, K., Student, S. P., ... Student, A. A. S. (2017). A ROBUST IMAGE WATERMARKING USING SVD AND DIFFERENTIAL EVOLUTION IN DWT DOMAIN, 1071–1074.
- [10] Abd, M., Aziz, E., Ewees, A. A., & Ella, A. (2017). Whale Optimization Algorithm and Moth-Flame Optimization for multilevel thresholding image segmentation, 83, 242–256. <https://doi.org/10.1016/j.eswa.2017.04.023>.