

Digital Signature based Image Watermarking using GA and PSO

R. Surya Prakasa Rao
Research Scholar,
Dept., of ECE,

AU College of Engineering, Visakhapatnam, India.

Prof. P. Rajesh Kumar
Professor & HOD,
Dept., of ECE,

AU College of Engineering, Visakhapatnam, India.

Abstract: This paper proposed a new digital image watermarking scheme based on Integer Wavelet transform and Singular value decomposition. The proposed approach adopts two metaheuristic algorithms such as Genetic Algorithm and Particle Swarm optimization for optimization purpose. For an enhanced authentication, a new signature generation and signature embedding procedure is also developed in this paper. The proposed signature generation and signature embedding procedure is completely based on the singular values. Various simulation tests are performed to reveal the Excellency of proposed approach and the obtained simulation results illustrates the efficiency of proposed approach.

Keywords: Image watermarking, IWT, SVD, GA, PSO, PSNR, NC.

I. INTRODUCTION

Recently, the vast increase in the pirated digital media due to the World Wide Web availability and the speed of distribution has led to the need to protect the media against attacks. The digital media (such as video, image, audio or text) can be modified easily by attackers who can then claim its ownership. So, owners, authors, publishers and providers of that media, are reluctant to grant the distribution of their documents in a networked environment [1]. The need to develop robust methods to protect the intellectual property rights of data owners against unauthorized copying, and redistributing it on the network became the main objective of researchers in digital watermarking. Traditional methods such as copy protection or encryption could not solve the problem of unauthorized copying entirely.

Digital watermarking presents a viable solution to that problem by marking the digital media, then it can be easy to be spread and later track it [1]. This can be referred to as a digital signature. The technology used to apply the digital signature on the digital media is called copyright protection. Digital watermarking is described as technologies and methods that hide information sometimes called a signal or watermark; for example, a number or text, into media files such as images, videos, audio, and text. A digital watermark can be visible or invisible to the human visual system. Logos that are often seen added to the corners of images or videos as a way to prevent copyright infringement is an example of visible digital watermark. These watermarks can be easily defeated and removed by replacing or cropping it from the digital media. As a result, the recent effort of research intends to develop watermarking systems to protect the media content. These systems should satisfy the imperceptibility, the robustness, the security and the capacity requirements.

According to the domain used for embedding, the current schemes of digital watermark are basically classified into two types [2]: (i) Spatial domain; (ii) Transform domain. The transform domain involves discrete Fourier transform (DFT), discrete cosine transform (DCT), and discrete wavelet transform (DWT), etc. Many related watermarking schemes have been proposed [3]. In recent years, the watermarking scheme, which is based on singular value decomposition (SVD), became a hot area during the watermarking procedures. In 2002, Liu and Tan [4] first proposed the SVD-based watermarking algorithm. In their scheme, the SVD transform is applied on the original image, and the watermark is embedded into the singular value matrix. Kamble *et al.* [5] presented a digital image watermarking method based on Arnold transform, SVD, and DWT. A watermark is encrypted with a secret key obtained by Arnold transform. The original image is decomposed by two-level wavelet transform, and the low resolution approximation matrix can be acquired. Then, the SVD transform is applied on the low frequency sub-band, and the encrypted watermark is embedded into the singular value matrix of the low frequency sub-band. Fazli and Moeini [6] proposed a robust hybrid image watermarking scheme using DWT, DCT, and SVD. In this method, the original image is partitioned into four areas: up-left, up-right, down-left, and down-right. Each area is decomposed by DWT. Then the coefficient matrix HL and LH are partitioned into 8×8 non-overlapping image blocks. DCT is performed on each block, and the coefficients in the location of (1, 2) and (2, 1) are obtained to organize a new matrix. After applying SVD on the new matrix, the singular value matrix of the new matrix is used as the embedded location of encrypted watermark. Ganic *et al.* [11] inserted the singular values of the gray scale watermark into the singular values of all one-level DWT sub-bands. Rastegar *et al.* [9] also suggested a hybrid watermarking scheme. They applied radon transform to the host image, then decomposed it into three levels using DWT. The singular values of the third-level DWT sub-bands are modified by the singular values of the binary watermark. Lagzian *et al.* [8] replaced DWT by RDWT and followed the same steps used by Ganic *et al.* [11]. These schemes performed well against some attacks, but their schemes have a weakness in the security because they applied SVD for the watermark in the embedding process [13, 14, 12]. Lai *et al.* [7] scheme could overcome this security issue. They decomposed the image using DWT, divided the watermark into two halves and then embedded each half into the singular values of LH and HL sub-bands of DWT transform of the

host image. Although, Lai et al. scheme fulfilled the requirements of digital image watermarking, their scheme's capacity is still insufficient.

In this paper, we met all the requirements of watermarking, especially robustness, embedding capacity and imperceptibility. Moreover we attempted to overcome the lack of security problem. Various approaches are proposed in earlier to investigate this issue. Loukha et.al [15] and guptha et.al [16] proposed two solutions to solve the security issue in image watermarking. The first solution [17] is applying a one-way hash function to the U and V. This gives the two hashing values HU and HV. Then the singular values are modified based on these hash values. [16] Proposed another solution to this problem. The authors proposed a signature based authentication mechanism for both U and V before continuing the extraction procedure. Based on Loukha and Guptha, [18] proposed a new solution for solving the security problem. In [18] the SHA-1 algorithm was applied on U and V to obtain two hashing values. Then a new result (R1) is generated by XORing them. In addition a new secret key is generated with the same dimensions of U and V. The final signature is obtained by XORing the result R1 and the binary version of secret key. A new procedure of singular values modification through the signature embedding procedure. Though this approach achieved an enhanced performance, there is no strict process of secret key generation and also didn't given any clarification about the band selection at signature embedding. One more issue with [18], 1-level DWT applied to host image which can't provide much information about the resolution levels of host image.

To overcome the problems with conventional approaches, this paper propose a new intelligent digital image watermarking scheme based on the 3-level Integer Wavelet transform (IWT), Normalized Singular Value Decomposition (NSVD) and a new signature generation and embedding procedure. The proposed approach also applies Genetic Algorithm (GA) and particle swarm Optimization for the optimization purpose. The simulation results are tested over various attack types to show the effectiveness.

Rest of the paper is organized as follows; section II gives the basic details about the technologies used in the proposed approach. Section III illustrates the complete details of proposed approach. Section IV gives the details of experimental results and finally the conclusions and future scope is provided in section V.

II. PRELIMINARIES

A. Normalized SVD (NSVD)

From the SVD point of view it was noticed that every image matrix has the well-known SVD for any given single matrix A, the larger Singular Values (SVs) are very sensitive to variations in the image such as noise changes in the host image. Upon the occurrence of attack on the watermarked image, there may be effect on the pixel intensities. But the SVD are very sensitive to these variations. To alleviate the variations in image, a normalized SVD approach is proposed with mainly two ideas such as the weights of host image uv^T should be deflated since they are every sensitive to the variations in the image itself and weights of base images uv^T corresponding to relatively small

λ_i 's should be inflated, since they may be less sensitive to the variations within the image.

This can be illustrated through the following concept. Let's consider the image I is denoted as $I = [i_1, i_2, \dots, i_r]^T$, where i_i^T is a $1 \times c$ row vector that represents the i_{th} row of matrix I, then

$$V^T C_{row} V = S^2 \quad (1)$$

Where

$$C_{row} = I^T I = \sum_{i=1}^r i_i i_i^T \quad (2)$$

I.e., v_j is the eigenvector of the covariance matrix C_{row} corresponding to Eigen value $\lambda_j^2, j = 1, 2, \dots, k$. Similarly, Let's consider the image I is denoted as $I = [i_1, i_2, \dots, i_c]^T$, where i_i^T is a $r \times 1$ row vector that represents the i_{th} Colom of matrix I, then

$$U^T C_{row} U = S^2 \quad (3)$$

Where

$$C_{row} = I^T I = \sum_{i=1}^r i_i i_i^T \quad (4)$$

I.e., u_j is the eigenvector of the covariance matrix C_{row} corresponding to Eigen value $\lambda_j^2, j = 1, 2, \dots, k$.

Hence, the λ_i 's should be inflated, since they may be less sensitive to the variations within the image, a new SVD formulation can be derived by modifying the standard SVD evaluation as,

$$A = US^{\gamma}V^T \quad (5)$$

Where U, S and V are the corresponding matrices, and γ is the normalizing constant. In order to achieve the requirements, the γ needs to satisfy the following condition.

$$0 \leq \gamma \leq 1 \quad (6)$$

B. Signature Generation Procedure

A new image authentication mechanism based on the several suggestions proposed in earlier [19, 20, 21] is suggested in this paper. The authors revealed that the flaws of the conventional approaches are due to the utilization of U and V matrices which preserves most significant information. If there is an availability of U and V along with the eigenvectors of S, the information loss in the reconstructed image will be less. When applying inverse SVD, eigenvectors play a significant role in the reconstruction process. Thus, any singular matrix S is used along with these eigenvectors, producing a correlated output instead of an actual output. The correlation will be high if the unmatched singular values are approximately equal to the original singular values, and hence, a security weakness arises, namely, the high probability of false positive watermark detection. This security threat is due to unauthorized embedding by an attacker, in which personal eigenvectors are employed in the extraction process to claim a false ownership. Thus, a signature-based authentication mechanism for the matrices U and V is proposed in this paper to overcome such drawbacks. The generation of signature considers the orthonormal matrices U and V. Secure Hashing Algorithm (SHA) is used here to generate the digests of U and V. By performing a bitwise XOR operation between the obtained digests of U and V an initial result R1 is formulated. Further a random secret key is generated with the same size of the R1. Here the secret key is completely random in nature. For every test case the nature of random key will vary. Then performing the XOR

operation between the random secret key and result R1 derives a new result R2. For the purpose of authentication, the first eight bits of R2 is chosen as a digital signature, sign.

C. Signature Embedding Procedure

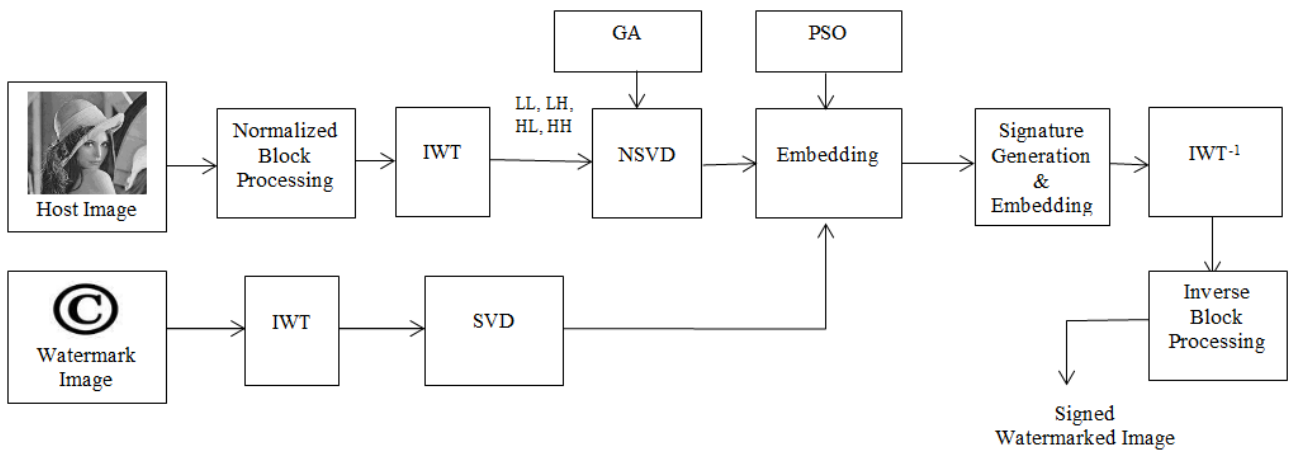
After the signature generation, it is embedded into the watermarked image in such way that it is robust to various attacks and also the degradation in the quality of image is less. The entire watermarked image is not considered for signature embedding. Only some portion of the watermarked image is considered for signature embedding. This some portion is selected based on the correlation between the image pixels. If the signature is embedded in the pixels with low correlation the attacker can break the security easily and can predict the further information based on the on one pixel. Thus the signature is embedded in the pixels with loss correlation such that the quality of I age also wont affected. The process of signature embedding is explained as follows:

1. Decompose the watermarked image using 1-DWT.
2. Divide the obtained approximation coefficients into 8*8 blocks.
3. Evaluate the correlation between the coefficients of every block and also the block correlations.
4. Find the first eight blocks with high correlation.

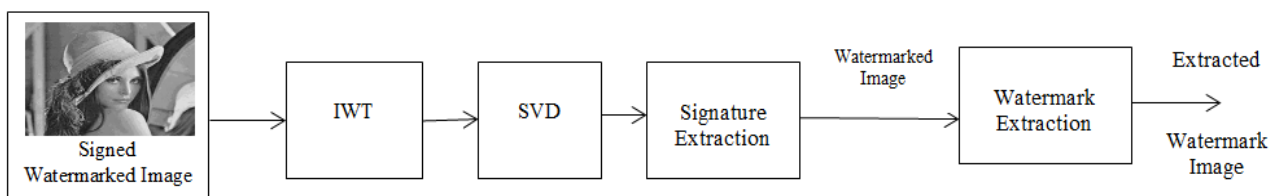
5. Perform SVD over every block.
6. Round off the obtained singular values to its nearest integers after scaling it with the factor of 10.
7. Modify the singular value according to the signature bits as follows;
 If the signature bit is equal to 1 and the modified singular value is even, or if the signature bit is equals to 0 and the modified singular value is odd, add one to the modified singular value and divide the results by a factor of 10.
 Else keep as is its.
8. Rearrange the all modified blocks in their respective positions such that the coefficient mismatching won't occur.
9. Perform inverse SVD for all the rearranged blocks.
10. Perform inverse DWT.

III. PROPOSED WATERMARKING SCHEME

The complete details of proposed signature based watermarking scheme is illustrated in this section. Total process is carried out in two phases, embedding and extraction. The block diagrams of embedding and extraction phases are shown in the figure.1 (a) and (b) respectively.



(a)



(b)

Figure.1 block diagram (a) Embedding (b) Extraction

A. Embedding Procedure

1. Choose one host image and apply normalized block processing.
2. Apply 3-level IWT over the normalized host image such that the obtained subbands approximations and details.

3. Apply SVD over all the bands obtained.
4. Choose one watermark image and apply IWT over it to get subbands followed by SVD.

5. Modify the singular values of host image by adding the watermark image with singular values after multiplying them with a watermarking constant, alpha.

6. Generate a digital signature and embed it in the watermarked image through the process specified in section II-C.

7. Apply inverse SVD, Inverse IWT and Inverse Block Processing to obtain the signed watermarked image.

B. Extraction Procedure

1. Apply IWT on the signed watermarked image such that the obtained coefficients are approximations and details.

2. Apply SVD over all the obtained bands.

3. Perform signature extraction form the modified singular values through the procedure exactly opposite to the process specified in section II-C.

4. Perform watermark extraction over the obtained watermarked image.

5. Evaluate peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC) between the original ad extracted watermark images.

6. Apply Genetic Algorithm and Particle Swarm Optimization in an iterative fashion until achieving the optimal fitness function. The fitness function is derived from NC as follows

$$fitness = 1 - Average(NC_j) \tag{7}$$

Where

$$NC_j = \frac{1}{n_{attack}} \sum_{k=1}^{n_{attack}} NC(w, w_j^{*,k}) \tag{8}$$

Where w is original watermark and $w_j^{*,k}$ represents the extracted watermark through the proposed approach characterized by the position of the j^{th} particle. The smaller fitness value means the better robustness. Here, n_{attack} signifies the number of attacks,

IV. SIMULATION RESULTS

The proposed waterarking approach was implemented using MATLAB. To test the proposed approach various test images are considreed and the size of host image is kept as 512*512 and the watermark image 64*64. The evaluation of the performance of proposed approach under various circumstances was conducted in terms of imperceptibility and robustness against various attacks. The most widely used criteria are the peak signal-to-noise ratio ($PSNR$) and the normalized correlation (NC), which are employed consecutively. The $PSNR$ is utilized to estimate the imperceptibility, a term used to evaluate the similarity between a host image and a water-marked image, and can be defined as follows:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (w(i, j) - w^*(i, j))^2 \tag{9}$$

Where

w =original watermark image

w^* = extracted watermark image

$$PSNR = 10 * \log(255^2 / MSE) \tag{10}$$

$$SSIM = \frac{\sum_i \sum_j w(i, j) \otimes w^*(i, j)}{\sum_i \sum_j (w(i, j))^2} \tag{11}$$

The test images considered for evaluation are shown in figure.2, below

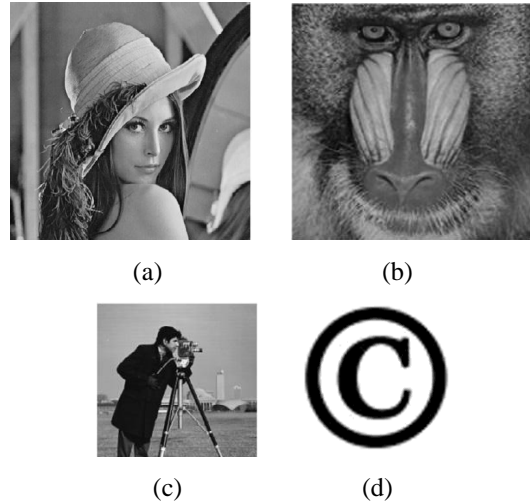


Figure.2 test imagery (a) Lena (b) Baboon (c) Cameramann (d) Logo

Various types of attacks are accomplished over the watermarked image to reveal the robustness of proposed scheme. To investigate the robustness of proposed approach, the watermarked image was subjected to eight attacks such as: (1) Gaussian noise Attack (GNA) (2) salt & pepper noise attack (SPA) (3) Median Filtering attack (MFA), (4) Histogram Equalization attack (HEA), (5) Rotation attack (RA) (6) Contrast Enhancemnet attack (CEA) (7) cropping attack (CA) and (8) Scalling Attack (SA). The obtained results for both no attack and attack scenarios is represnted below.



Figure.3 obtained results under no attack scenario (a) Signed Watermarked image (b) Extracted Watermark

In this test case, the signed watermarked image is not subjected to any attack. The signed watermarked image is passed to extraction unit as it is without any modification and for the extracted watermark, the performance metrics are evaluated. In the case of attack scenario, the signed watermaekd image is subjected to attacks an dthe it is passed to extraction unit to reveal te performance of proposed approach. Further the obtained results of watermarked image and the extracted image are shown in the following figures.

A. Gaussian Noise

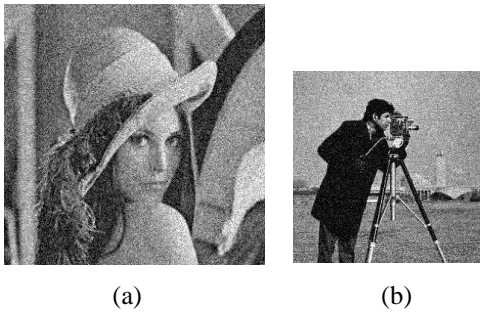


Figure.4 (a) Watermarked Image (b) Extracted Watermark

B. Salt & Pepper Noise

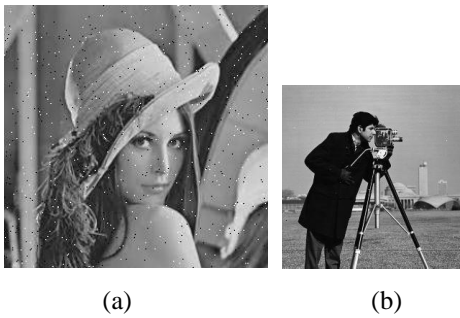


Figure.5 (a) Watermarked Image (b) Extracted Watermark

C. Median Filter



Figure.6 (a) Watermarked Image (b) Extracted Watermark

D. Histogram Equalization



Figure.7 (a) Watermarked Image (b) Extracted Watermark

E. Rotation

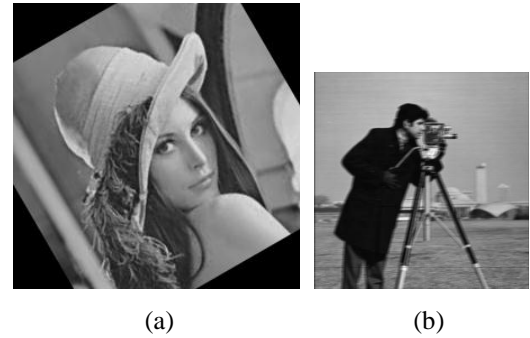


Figure.8 (a) Watermarked Image (b) Extracted Watermark

F. Contrast Enhancemnet



Figure.9 (a) Watermarked Image (b) Extracted Watermark

F. Cropping

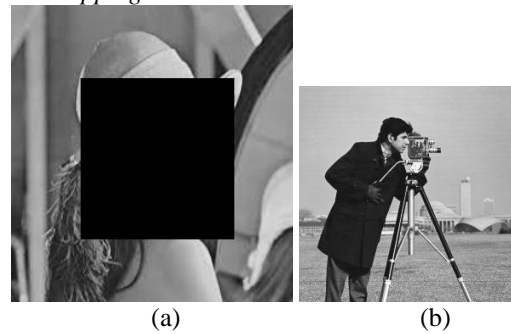


Figure.10 (a) Watermarked Image (b) Extracted Watermark

G. Scaling



Figure.11 (a) Watermarked Image (b) Extracted Watermark

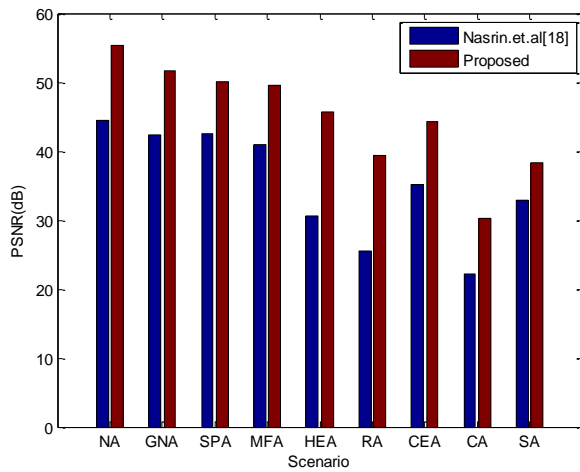
Here initially the Cameramann image is embedded in the Lena image and the obtained MSE, PSNR, NC and the SSIM for both attack and no-attack cases are represneted in table.1. Similarly the logo image is embedded in the baboon image and its respective results are represented in table.2.

Table.1 Performance metrics for the test case of Lena and Cameramann Image

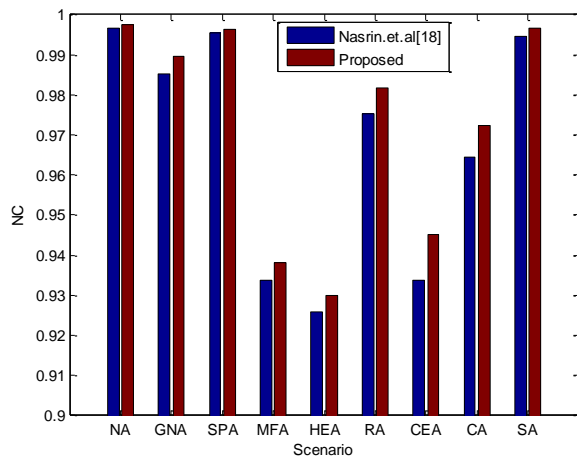
Attack	Nasrin et.al [18]				Proposed Approach			
	MSE	PSNR	NC	SSIM	MSE	PSNR	NC	SSIM
NA	2.2772	44.5568	0.9967	0.9822	0.1905	55.3326	0.9974	0.9908
GNA	3.8015	42.3312	0.9852	0.9645	0.4355	51.7412	0.9895	0.9796
SPA	3.6539	42.5032	0.9955	0.9447	0.6319	50.1244	0.9964	0.9586
MFA	5.1345	41.0258	0.9338	0.9412	0.7077	49.6321	0.9383	0.9552
HEA	57.2282	30.5547	0.9258	0.9333	1.7373	45.7823	0.9299	0.9444
RA	185.556	25.4458	0.9752	0.8724	7.5828	39.3325	0.9817	0.8899
CEA	19.9664	35.1278	0.9338	0.9323	2.4614	44.2189	0.9452	0.9598
CA	389.502	22.2257	0.9645	0.8552	60.1817	30.3358	0.9723	0.8645
SA	33.5483	32.8741	0.9947	0.9631	9.5706	38.3214	0.9966	0.9828

Table.2 Performance metrics for the test case of Lena and Logo Image

Attack	Nasrin et.al [18]				Proposed Approach			
	MSE	PSNR	NC	SSIM	MSE	PSNR	NC	SSIM
NA	1.2018	47.3325	0.9920	0.9813	0.2009	55.1010	0.9962	0.9941
GNA	1.8721	45.5132	0.9824	0.9645	0.4875	51.2513	0.9869	0.9805
SPA	2.5228	44.1120	0.9902	0.9447	0.6338	50.1111	0.9913	0.9586
MFA	3.6079	42.5582	0.9377	0.9423	0.9989	48.9842	0.9593	0.9555
HEA	66.5933	29.8965	0.9238	0.9339	2.1821	44.7421	0.9279	0.9445
RA	84.6702	28.8535	0.9795	0.8878	3.8898	42.2315	0.9804	0.9366
CEA	15.5453	36.2148	0.9373	0.9489	1.7164	45.7845	0.9422	0.9709
CA	172.119	25.7725	0.9712	0.8557	31.6673	33.1247	0.9747	0.8757
SA	26.5601	33.8885	0.9902	0.9689	5.3036	40.8851	0.9923	0.9833



(a)



(b)

Figure.12 Comparative analysis for the test of Lena with Cameramann image with reference to (a) PSNR (b) NC

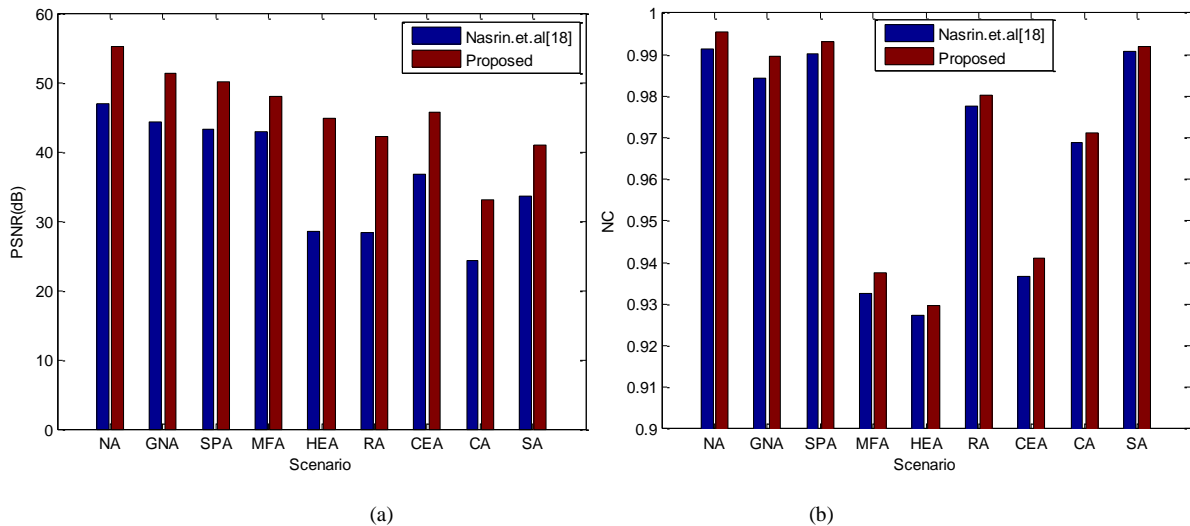


Figure.13 Comparative analysis for the test of Lena with Logo image with reference to (a) PSNR (b) NC

Figure.12 illustrates the performance of proposed approach under various test cases for a given Lena host and Cameramann watermark image. The PSNR is observed to be high for the proposed approach compared to the conventional one for the both attack and no-attack scenarios. Since there is optimization at both feature extraction level and also embedding phase, the quality of image is preserved in an efficient manner. Along with the PSNR, the NC also observed to be high for the proposed approach compared to the conventional approach. Since the proposed approach adopts a new signature based authentication mechanism the watermarked image is more robust to all types of attacks. Similarly figure.13 reveals the performance of proposed approach for the test case of Lena with logo image. For this case also the proposed approach is said to be achieved better results compare to conventional approach.

V. CONCLUSIONS

In this paper a new secure image watermarking approach is proposed to enhance the security of multimedia images during their transmission. Here the proposed approach achieved an excellent performance and outperforms the conventional approaches. Various test scenarios conducted over various images revealed the enhanced performance of proposed. Approximately the PSNR of proposed approach is increased by 8dB. Under simulation the proposed approach was analyzed by adopting various attack scenarios. From the results the proposed approach is revealing an excellent performance.

VI. REFERENCES

- [1] T. Hai, C. M. Li, J. M. Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: A Review," *Journal of Applied Research and Technology*, vol. 12, no. 1, pp. 122-138, Feb. 2014.
- [2] X. Y. Ye, X. T. Chen, M. Deng, S. Y. Hui, and Y. L. Wang, "A multiple-level DCT based robust DWT-SVD watermark method," in: *Proceedings of the 10th International Conference on Computational Intelligence and Security*, Kunming, China, Nov. 15-16, 2014, pp. 479-483.
- [3] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, "Watermarking techniques used in medical images: A survey," *Journal of Digital Imaging*, vol. 27, no. 6, pp. 714-729, Dec. 2014.
- [4] R. Z. Liu and T. N. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 121-128, Mar. 2002.
- [5] S. Kamble, V. Maheshkar, S. Agarwal, and V. K. Srivastava, "DWT-SVD based robust image watermarking using Arnold map," *International Journal of Information Technology and Knowledge Management*, vol. 5, no. 1, pp. 101-105, Jan.-Jun. 2012.
- [6] S. Fazli and M. Moeini, "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks," *Optik*, vol. 127, no. 2, pp. 964-972, Jan. 2016.
- [7] Lai CC, Tsai CC. Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Trans Instrum Meas* 2010;59(11):3060-3.
- [8] Lagzian S, Soryani M, Fathy M. A new robust watermarking scheme based on RDWT-SVD. *IJIP Int J Intell Inform Process* 2011;2(1):22-9.
- [9] Rastegar S, Namazi F, Yaghmaie K, Aliabadian A. Hybrid watermarking algorithm based on singular value decomposition and radon transform. *Int J Electron Commun (AEU)* 2011;65(7):658-63.
- [10] Bhatnagar G. A new facet in robust digital watermarking framework. *International Journal of Electronics and Communications (AEU)* 2012;66(4):275-85.
- [11] Ganic E, Eskicioglu AM. Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. *J Electron Imaging* 2005; 14(4):043004-9.
- [12] Lai CC. An improved SVD-based watermarking scheme using human visual characteristics. *Optical Communications* 2011;284(4):938-44.
- [13] Ling HC, Phan RCW, Heng SH. On the security of a hybrid watermarking algorithm based on singular value decomposition and radon transform. *Int J Electron Commun (AEU)* 2011;65(11):958-60.
- [14] Zhang XP, Li K. Comments on "an SVD-based watermarking scheme for protecting rightful ownership". *IEEE Trans Multimedia* 2005;7(3): 593-4.
- [15] Khaled Loukhaoukha, Jean-Yves Chouinard, M. Haj Taieb, Optimal image watermarking algorithm based on LWT-SVD via multi-objective ant colony optimization, *J. Inf. Hiding Multimed. Signal Process.* 2 (2011) 303-319.
- [16] A. Gupta, M. Raval, A robust and secure watermarking scheme based on singular values replacement, *Sadhana* 37 (2012) 425-440.
- [17] K. Loukhaoukha, J.Y. Chouinard, Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification, in: *Canadian Work-shop on Information Theory*, 2009, pp.177-182.
- [18] Nasrin M.Makbol, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition", *Digital Signal Processing* 33 (2014) 134-147.

- [19] X.P. Zhang, K. Li, Comments on “An SVD-based watermarking scheme for protecting rightful ownership”, IEEE Trans. Multimed. 7(3) (2005) 593–594.
- [20] H.C. Ling, R.C.W. Phan, S.H. Heng, On the security of a hybrid watermarking algorithm based on singular value decomposition and radon transform, AEU, Int. J. Electron. Commun. 65(11) (2011) 958–960.
- [21] R. Rykaczewski, Comments on “An SVD-based watermarking scheme for protecting rightful ownership”, IEEE Trans. Multimed. 9(2) (2007) 421–423.