International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

IMPLEMENTATION OF IMAGE AUTHENTICATION USING DIGITAL WATERMARKING WITH BIOMETRIC

D HARIKA[1], SYED NOORULLAH[2]
[1]DECS 202T1D3803, ASHOKA WOMENS ENGINEERING COLLEGE, KURNOOL, A.P.
[2]Assistant Professor – ASHOKA WOMENS ENGINEERING COLLEGE, KURNOOL, A.P

ABSTRACT
The rapid global development of E-commerce in terms of digitalization and distribution of digital contents in the form of image, audio, video, increases the possibility of unrestricted duplication and broadcasting of copyrighted data and the protection of crucial documents is highly significant. Digital watermarking inserts watermark into the cover or host data by unnoticeable modification. In this work digital watermarking with biometric features is done. In this work a technique to implement the hiding of an image inside another image using biometric features namely signature and fingerprint using watermarking techniques is done. To accomplish this, a hybrid watermarking scheme consisting of Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition (DWT-DCT-SVD) is proposed for image authentication that is robust against attacks. Here, singular values of watermark1 (fingerprint) and watermark2 (signature) are obtained by applying DWT-DCT-SVD. By adding both the singular values of watermarks we acquire the transformed watermark. To improve the security, robustness and provide authenticity for the image, a two-step watermarking method is demonstrated. The evaluation parameters like PSNR (Peak Signal to Noise Ratio), SSIM (Structured Similarity Index Method), normalized correlation coefficient (NCC) are used for image quality assessment.

Key Words - Singular value decomposition, Normalized Cross Correlation and Peak Signal to Noise Ratio, Discrete Wavelet Transform, Discrete Cosine Transform.

1. Introduction

The concept of biometric watermarking is used for advanced security of biometrics. Watermarking techniques have been used in biometric systems for the purpose of protecting and authenticating biometric data and enhancing accuracy of recognition. The transform domain techniques used are DWT, DCT and SVD. The DCT transform is mainly used to compress the data or image. DWT decomposes an image into a set of four non-overlapping multi-resolutions. The SVD of a matrix is orthogonal transforms used for matrix diagonalization. Watermarking embedding can be done with each of the above-mentioned techniques, but each one has some drawbacks with regards to some attacks. So, in order to overcome these drawbacks, we integrate all three techniques and make a hybrid system which is more robust and secure. This hybrid model withstands different image processing attacks. Thus, the final result does not change even after applying the attacks. Therefore, we can say this technique improves the security without altering the existing image data properties to a great extent. Rapid evolution of digital technology has improved the ease of access to digital information. Digitizing of multimedia data has enabled reliable, faster and efficient storage, transfer and processing of digital data. It also leads to the consequence of illegal production and redistribution of digital media. Duplication and modification of such digital data has become very easy and undetectable. Hence the risk of copyright violation of multimedia data has increased due to the enormous growth of computer networks that provides fast and error free transmission of any unauthorized duplicate and possibly manipulated copy of multimedia information. One way to protect multimedia data against illegal recording and distribution is to embed a secondary signal or pattern into the image, video or audio data that is not perceivable and is mixed so well with the original digital data that it is inseparable and remains unaffected against any kind of multimedia signal processing. This embedded secondary information is digital watermark which is, in general, a visible or invisible identification code that may contain some information about the intended recipient, the lawful owner or author of

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

the original data, its copyright etc. in the form of textual data or image. The information to be hidden is embedded by manipulating the contents of the digital data, allowing someone to identify the original owner, or in the case of illegal duplication of purchased material, the buyer involved. This digital watermark can be detected or extracted later to make an assertion about the data. Digital watermarks remain intact under transmission / transformation, allowing us to protect our ownership rights in digital form. Absence of a watermark in a previously watermarked image would lead to the conclusion that the data content has been modified. In order to be effective for copyright protection, digital watermark must be robust, recoverable from a document, provide the original information embedded reliably, and be non-intrusive and also removable by authorized users. Robust watermarks are those which are difficult to remove from the object in which they are embedded despite a variety of possible attacks by pirates including compression such as JPEG, scaling and aspect ratio changes, rotation, translation, cropping, row and column removal, addition of noise, filtering, cryptographic and statistical attacks, as well as insertion of other watermarks. Here cryptographic techniques and statistical properties of pseudo-random numbers play an important role. DWT produces four sub-bands low-low (LL), low-high (LH), high-low (HL) and high-high (HH). By using these four sub-bands we can regenerate the original image. Theoretically, a filter bank shown in Fig. 1 should work on the image in order to generate different sub-band frequency images.

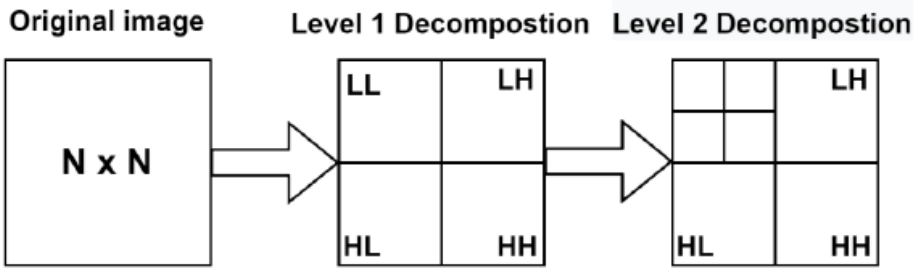

Fig.1. Sub-bands resulting after 2-level decomposition

As shown in fig.2 The LL sub-band specifies low-pass filtering on each row and each column, and it is a low-resolution approximation of the original image. Similarly, the LH sub-band resulted from the low-pass filtering on each row and the high-pass filtering on each column. The high-frequency details along the column direction influence the LH sub-band. The HL sub-band is the result of high-pass filtering on each row and the low-pass filtering on each column. The high-frequency details along the row direction influence the HL sub-band. The HH sub-band is constructed from the high-pass filtering on each row and each column. The high-frequency details along the diagonal direction influence the HH sub-band.

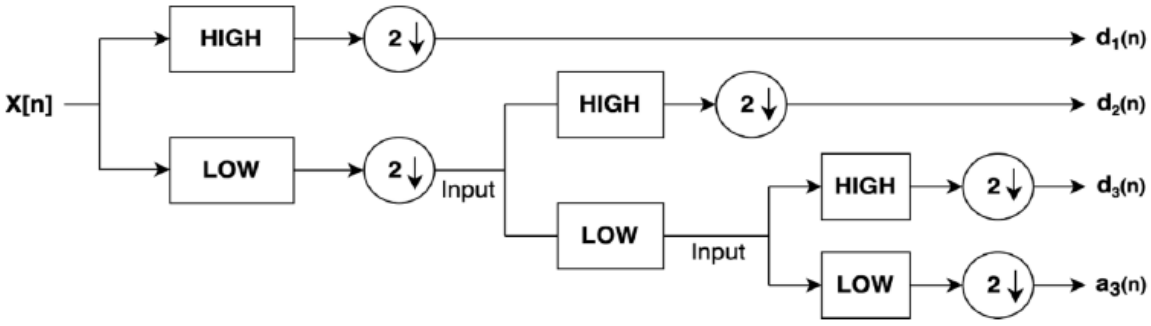

Fig.2. Block diagram of the 2 level DWT scheme

DWT Based Feature Extraction: DWT performs multi-level decomposition of the pre-processed image which results in efficient extraction of discriminant features which are insensitive to arbitrary environmental variations.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

DWT is a wavelet transform for which the discrete interval wavelets are sampled. DWT gives an image's simultaneous frequency and spatial domain information. In DWT operation, combination of analysis filter bank and decimation operation an image can be analysed. A pair of low and high pass filters corresponding to each decomposition level is the composition of the analysis filter bank. Approximate information of the image is extracted by a low pass filter whereas the details such as edges are extracted by high pass filter.

SVD:

Singular Value Decomposition (SVD) is used to approximate the matrix decomposition of the data into an optimal estimate of the signal and the noise components. This property is one of the most important properties of the SVD decomposition in noise filtering, compression and forensic which could also be treated as adding noise in a proper detectable way.

SVD refactors into three matrices for the given digital image. To refactor the image singular values are used and at the end of this process storage space required by the image is reduced as the image is represented with a smaller set of values. The SVD of mxn matrix A is given by the formula, SVD = u vT w

Where,

U: mxn matrix of the orthonormal eigenvectors of AAT.

VT: transpose of a n x n matrix containing the orthonormal eigenvectors of A^{T}A.

W: a nxn diagonal matrix of the singular values which are the square roots of the eigenvalues of ATA.

In linear algebra the SVD is a factorization of a rectangular real or complex matrix analogous to the diagonalization of symmetric or Hermitian square matrices using a basis of eigenvectors. SVD is an effective and most stable method to split the system into a set of linearly independent components, each of them bearing their own energy contribution [1,3]. A digital Image X of size MxN, with M ≥ N, can be represented by its SVD as follows:

Where U is a MxM orthogonal matrix, V is a NxN orthogonal matrix, and S is aMxN matrix with the diagonal elements representing the singular values, si of X. The transpose of the matrix is denoted by subscript T. The orthogonal matrix U columns are called the left singular vectors, and the orthogonal matrix columns V are called the right singular vectors.

Several SVD properties are highly advantageous for images such as; its maximum energy packing, solving of least squares problem, computing pseudoinverse of a matrix and multivariate analysis [1,2]. The relation to the rank of a matrix and its ability to approximate matrices of a given rank is a key property of SVD. Digital images are often represented by low rank matrices and, therefore, are able to be described by a sum of a relatively small set of eigen images.

Image Compression SVD with the maximum energy packing property is usually used in compression. As mentioned above, SVD decomposes a matrix into orthogonal components with which optimal sub rank approximations may be obtained [5, 14]. Significant savings in storage over storing the whole matrix with accepted quality offered by truncated SVD transformation with rank r. Figure shows the block diagram of the SVD based compression.

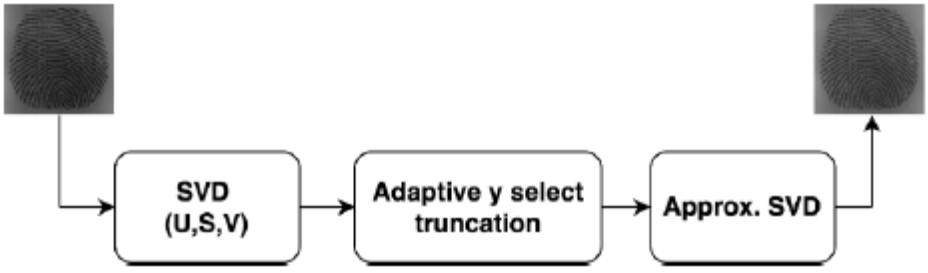

Fig 3. SVD block diagram

DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

First, the singular value matrix obtained by SVD contains illumination information. Therefore, changing the singular values will directly affect the illumination of the image. Hence, the other information in the image will not be changed. Second, by applying the illumination enhancement in LL subband will protect the edge information in other sub-bands (i.e. LH, HL, and HH).

2. Literature Survey

1."A robust blind colour image watermarking based on Fourier transform domain" published in 2020 used colour images watermarking based on the Fourier transform in a frequency domain technique to achieve good imperceptibility and also to generate watermarking images robust against various attacks with a high-quality watermark. The author Kahlessenane Fares et al., concludes saying the watermark into the higher coefficients can produce severe distortion of the image, whereas integrating into the lower coefficients makes the watermark robust to compression and filtering.

2. The author JUNXIU LIUet al., worked on watermarks with different sizes and proposed a image water -marking method that can achieve a good invisibility and robustness. Paper titled "An Optimized Image Watermarking Method Based on HD and SVD in DWT Domain" published in 2019.here the attacks were shown using graphs and plots.

3. Method of digital watermarking based on DWT-DCT-SVD was proposed using a scale factor and Arnold Transformation in the paper titled "A Proposed Digital Image watermarking Based on DWT-DCT-SVD" published in the year 2018 by Yuqi He.et al. Technologies used in the paper are Arnold Transform, discrete Wavelet Transform, discrete Cosine transform, singular value decomposition. In this paper, a method of digital watermarking based on DWT-DCT-SVD was proposed using a scale factor and Arnold Transformation in YUV Colour space. Proposed algorithm can be even more improvised to increase the robustness and imperceptibility.

4. The review of all existing steganographic methods (data embedding and extracting) for data hiding inside the text, image, audio and video channels have been described by the author Himanshu Arora et al., in the paper "Comparative study of image steganography techniques"

5. The paper titled "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection" published in 2017 by Durgesh Singh et al. Here the proposed
is free from false positive detection problems which occur in the SVD based watermarking schemes.

6. Another paper titled "Implementation of DCT DWT SVD based watermarking algorithms for copyright protection" published in 2015. The author A.B. Nandurbarkar et al., concludes that DWT is not robust against low pass filter attacks. DCT gives quite better results in all listed attacks. Here the comparative analysis of various Image compression techniques for different images is done based on three parameters: compression ratio (CR), mean square error (MSE), peak signal to noise ratio (PSNR).

7. The algorithm used in the paper "An optimized watermarking technique based on self-adaptive DE in DWT-SVD transform domain" published in 2014 has prominent imperceptibility and good robustness. The technology used here was an image watermarking scheme using self-adaptive differential evolution (SDE) algorithm based on optimal discrete wavelet transform–singular value decomposition (DWT–SVD) by author Mussrat Ali et al.

8. The paper titled "A Comparative Study of DCT, DWT & Hybrid (DCT-DWT) Transform" published in the year 2013 achieved higher compression ratio using Hybrid technique but loss of information is more. Here the author Archana Deshlahra et al., also describes that DWT requires more processing power and DCT overcomes this disadvantage since it needs less processing power, but it gives less compression ratio.

9. An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients. Ferda Ernawan, Dhani Ariatmanto, & Ahmad Firadus have published this journal in the year 2021. This paper proposed the adaptive scaling factor based selected DWT-DCT coefficients of its image content. The adaptive scaling factor was generated based on the role of selected DWT-DCT coefficients against the average value of DWT-DCT coefficients.

10. A DWT based watermarking approach for medical image protection. Fares Kahlessenane, Amine

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

Khaldi, Redouane Kafi, & Salah Euschi have published this paper in 2021. A discrete wavelet transform is applied to the image before the integration process, then, a topological reorganization of the coefficients of the LL sub-bands is done by the ZigZag scanning method. The obtained coefficients are then combined to integrate the watermark bits. A hash of the electronic patient record being integrated in the image, the integrity of the watermark can easily be verified. After the evaluation of our approach in terms of invisibility and robustness, the experimental results obtained show that our approach offers excellent imperceptibility.

11. Hybrid SVD-Based Image Watermarking Schemes: A Review published in 2021 by wafa hamdan alshoura, zurinahni zainol, je sen teh ,moatsum alwida, and abdullatif al abdullatif. There are many existing hybrid SVD-based image watermarking schemes found to be insecure. As there is also a lack of in-depth reviews in this domain, the focus of this paper is the analysis of the state-of-the-art in hybrid SVD-based image watermarking. We perform efficiency comparisons to highlight various security problems, open issues, and research gaps. Based on our findings, we additionally provide some recommendations for the development of more robust schemes in the future, This paper provides essential information for researchers and practitioners alike to advance the field of image watermarking.

Implementation

Figure 4 shows proposed implementation

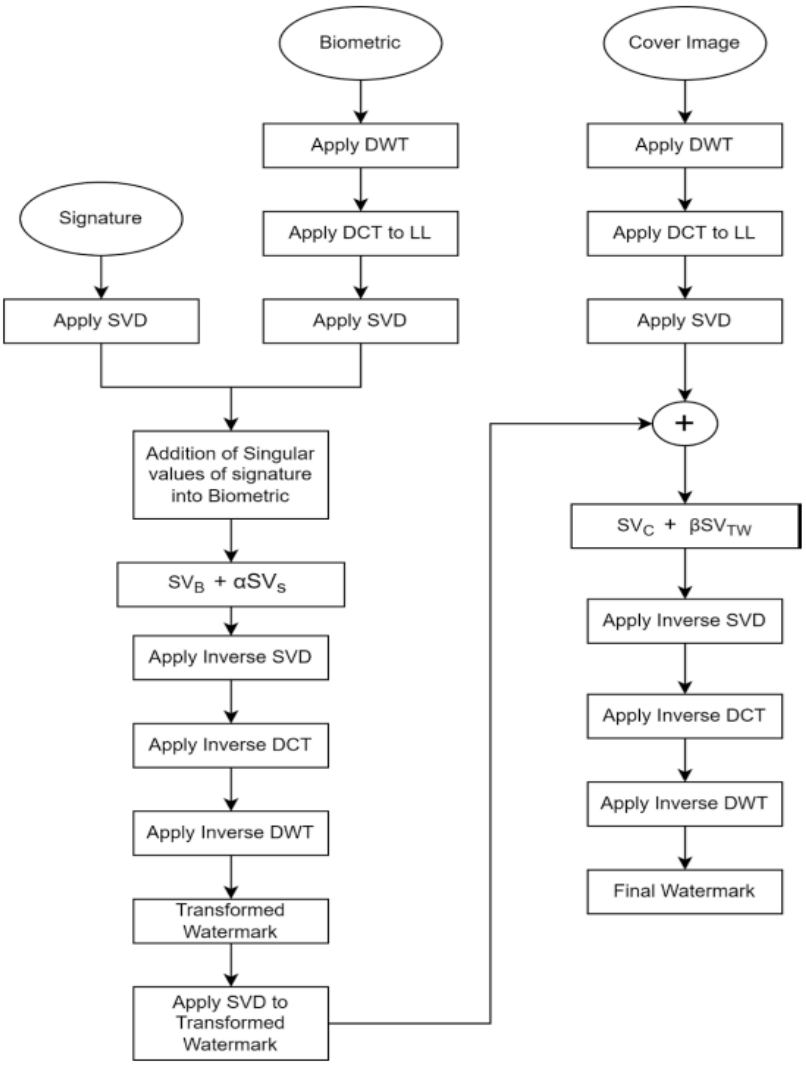

Fig 4. Proposed Design.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

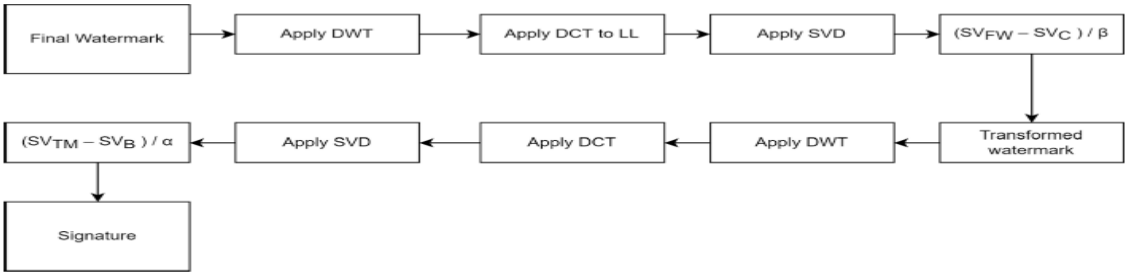

Fig 5. Proposed Design Extraction

Table 1: NCC values

ATTACKS	NCC_B	NCC_S
CROP	0.4345	0.9922
SALT & PEPPER	0.7586	0.7862
GUASSIAN	0.7472	0.7002
SPECKLE	0.4865	0.8047
ROTATION	0.5005	0.8827
SCALE 2X	0.9590	0.9340
SCALE 0.5X	0.6307	0.7165
MEDIAN	0.9650	0.9751
SHARPENING	0.5507	0.6234
MOTION BLUR	0.6217	0.8421
AVERAGE FILTER	0.62	0.8090
HISTOGRAM EQUALIZATION	0.6012	0.6104
JPEG	0.857	0.846
JPEG2000	0.846	0.8562

Table 1 depicts Normalised Cross Correlation (NC) values for biometric (NCCB) and signature (NCCS) under different types of attacks. In all the test cases the result obtained with better NCC values even after the extraction of watermarks viz, biometric and signature.

Table 2: PSNR

ATTACKS	$PSNR_B$	$PSNR_S$
CROP	4.1422	23.5847
SALT & PEPPER	5.2669	6.9213
GUASSIAN	6.8711	7.3798
SPECKLE	5.4516	11.4783
ROTATION	9.0110	7.2282
SCALE 2X	24.0391	17.1220
SCALE 0.5X	5.5592	7.5178
MEDIAN	6.6279	7.2673
SHARPENING	4.7371	9.6499
MOTION BLUR	4.3715	7.5336
AVERAGE FILTER	4.3984	7.8970
HISTOGRAM EQUALIZATION	5.4978	10.2860
JPEG	5.4542	9.5644
JPEG2000	6.4532	10.8961

Table 2 shows Peak Signal to Noise Ratio (PSNR) values for biometric (PSNRB) and signature (PSNRS) under different types of attacks. In all the test cases the result obtained with better PSNR values even after the extraction of watermarks viz, biometric and signature.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

Table 3: SSIM

ATTACKS	$SSIM_B$	$SSIM_S$
CROP	0.87634	0.90724
SALT & PEPPER	0.99536	0.76606
GUASSIAN	0.46688	0.55715
SPECKLE	0.78373	0.84695
ROTATION	0.78654	0.49736
SCALE 2X	0.98742	0.97214
SCALE 0.5X	0.99146	0.98632
MEDIAN	0.097755	0.36953
SHARPENING	0.32219	0.26843
MOTION BLUR	0.14037	0.049129
AVERAGE FILTER	0.12215	-ve
HISTOGRAM EQUALIZATION	0.29474	0.50328
JPEG	0.9519	0.94418
JPEG2000	0.80577	0.84715

Table 3 depicts Structural Similarity Index Metrics (SSIM) values for biometric (SSIMB) and signature (SSIMS) under different types of attacks. In all the test cases the result obtained with better SSIM values even after the extraction of watermarks viz, biometric and signature

.

RESULTS

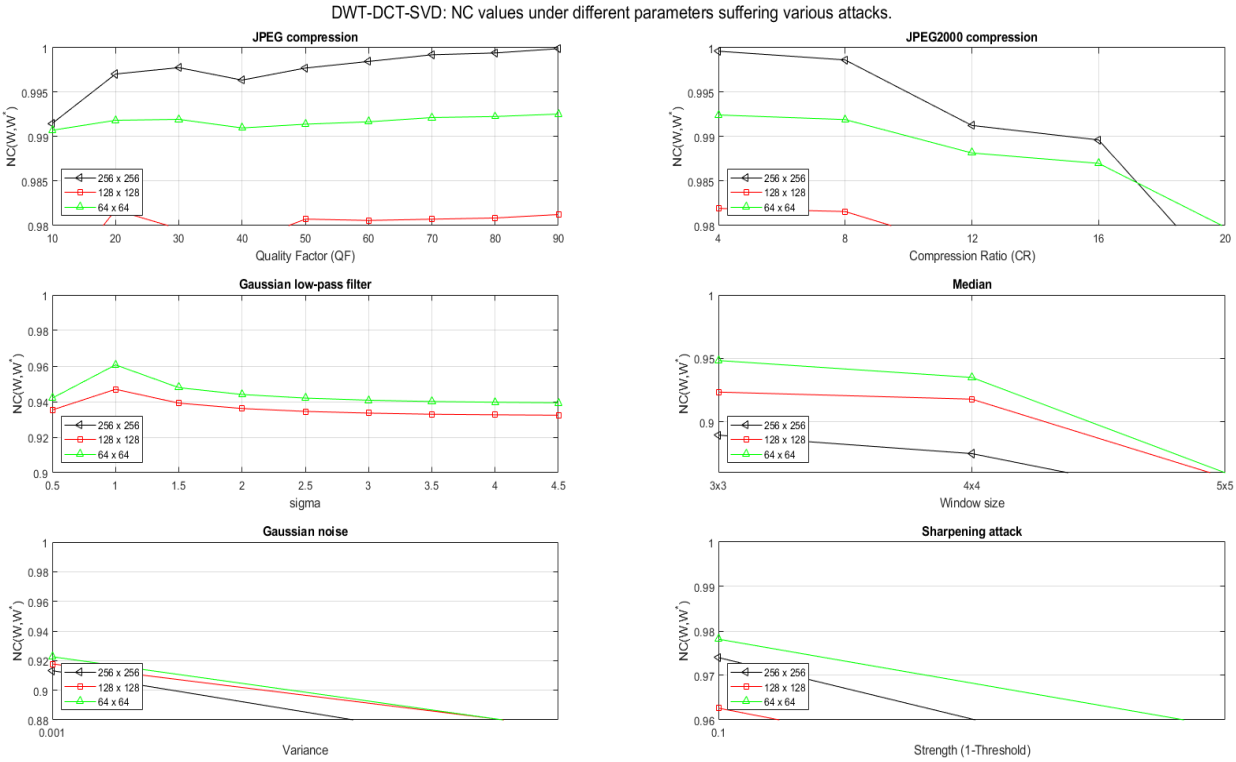

Fig 6. Various Parameters with different attacks

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

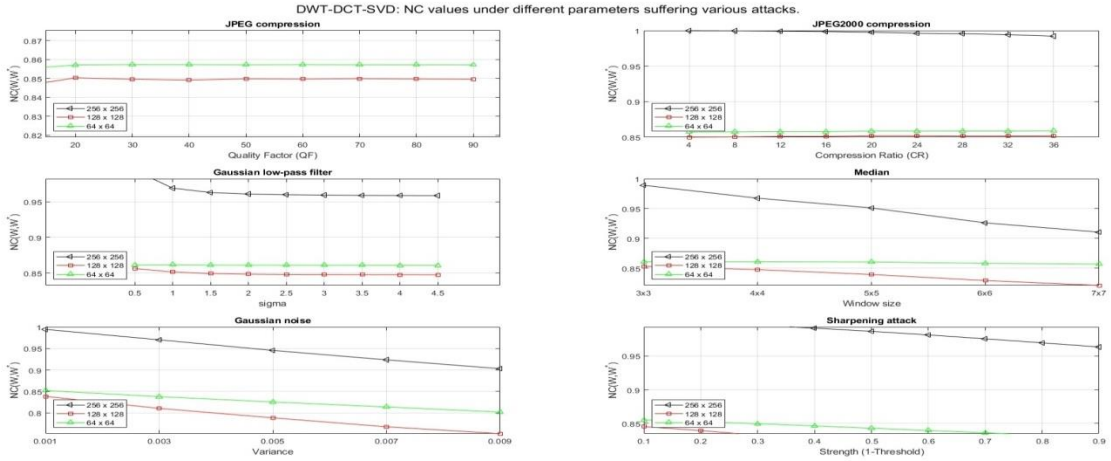

Fig 7. DWT-DCT-SVD NC values with different attacks

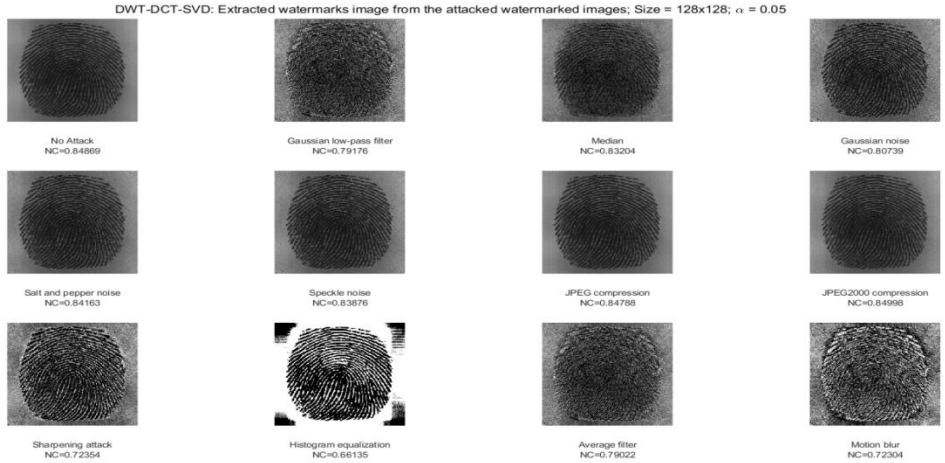

Fig 8 Biometrics 128x128 size with different attacks.

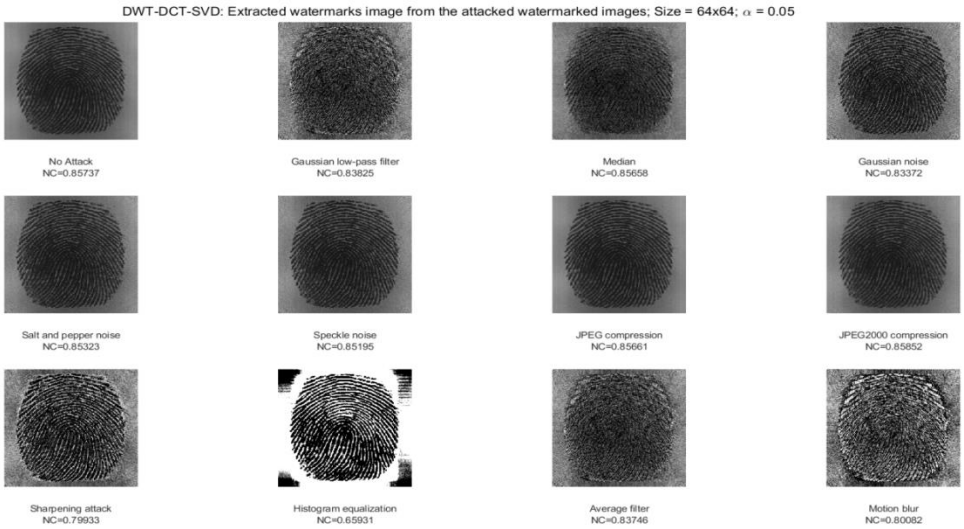

Fig 9 Biometrics 64x64 size with different attacks.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

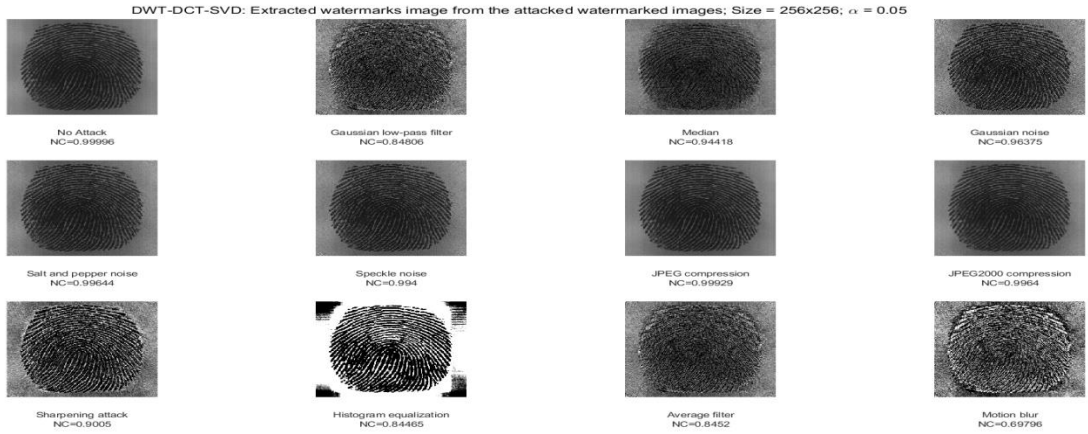

Fig 10. Biometrics 256x256 size with different attacks.

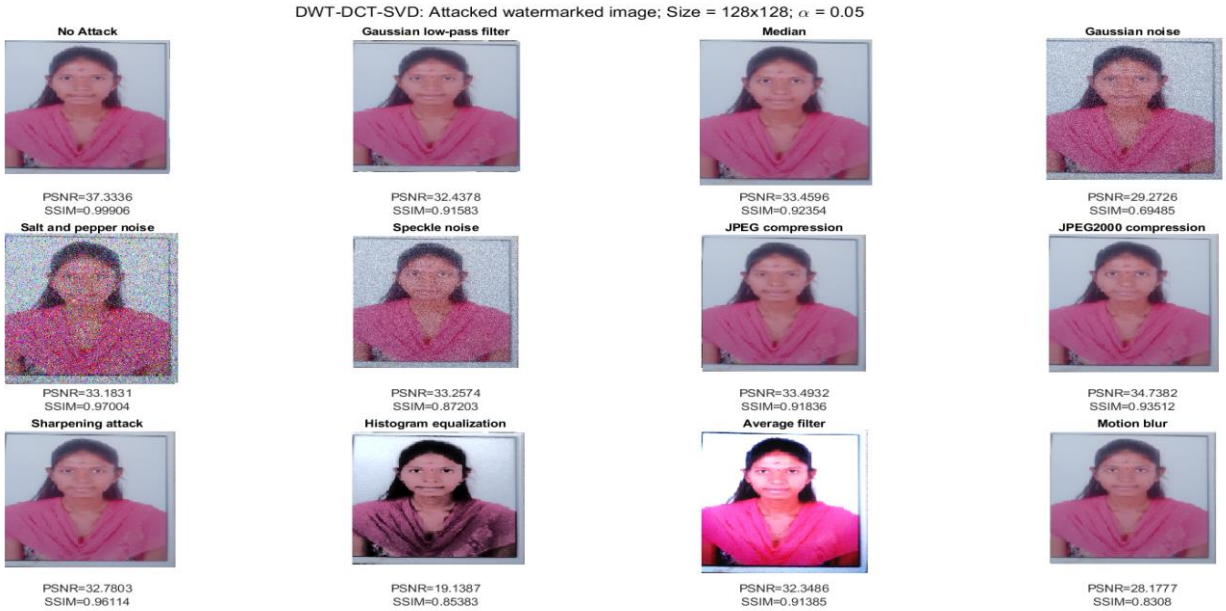

Fig 11 Attacked watermarked image of size 128x128.

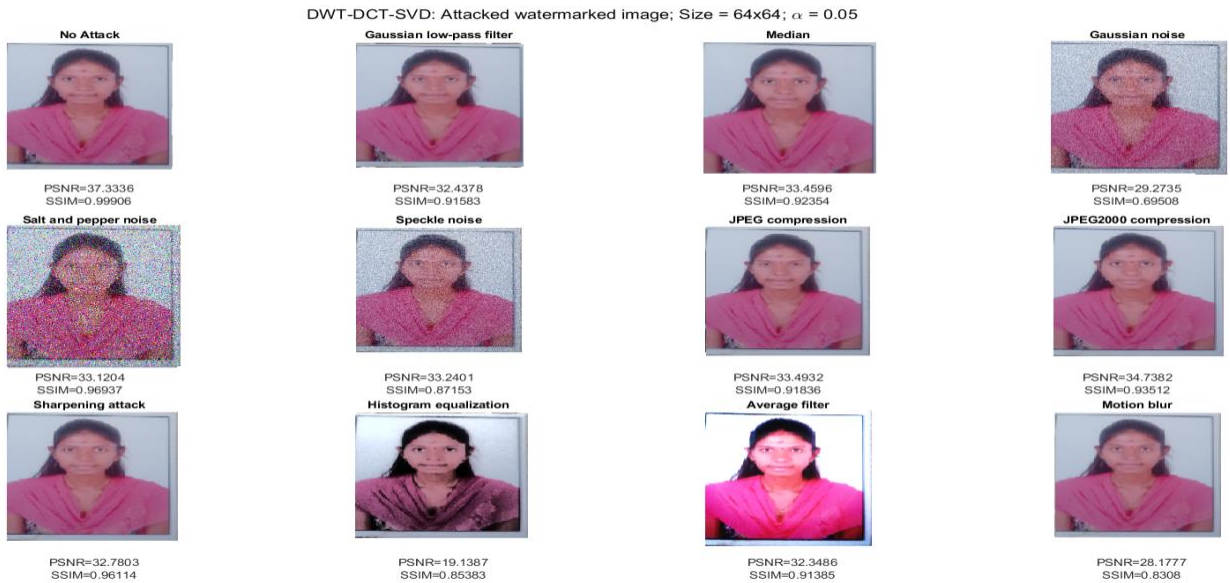

Fig 12 Attacked watermarked image of size 64x64.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

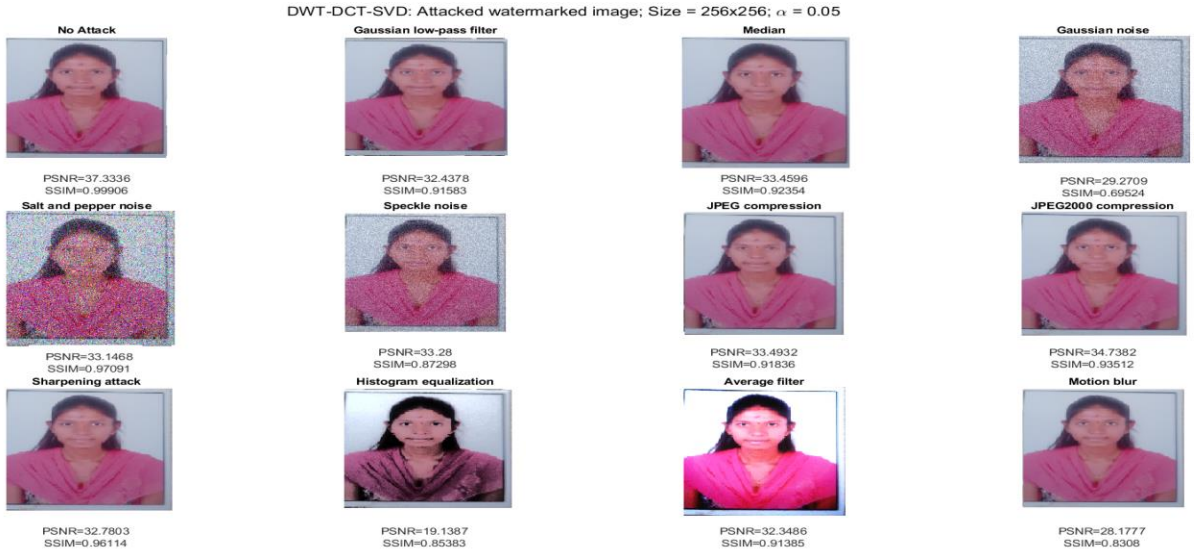

Fig 13 Attacked watermarked image of size 256x256.

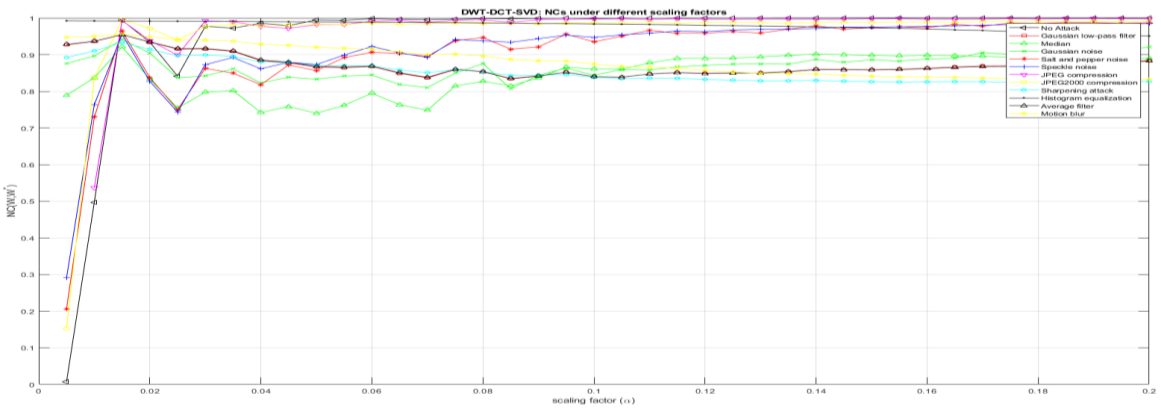

Fig 14 Scaling factor α vs NC.

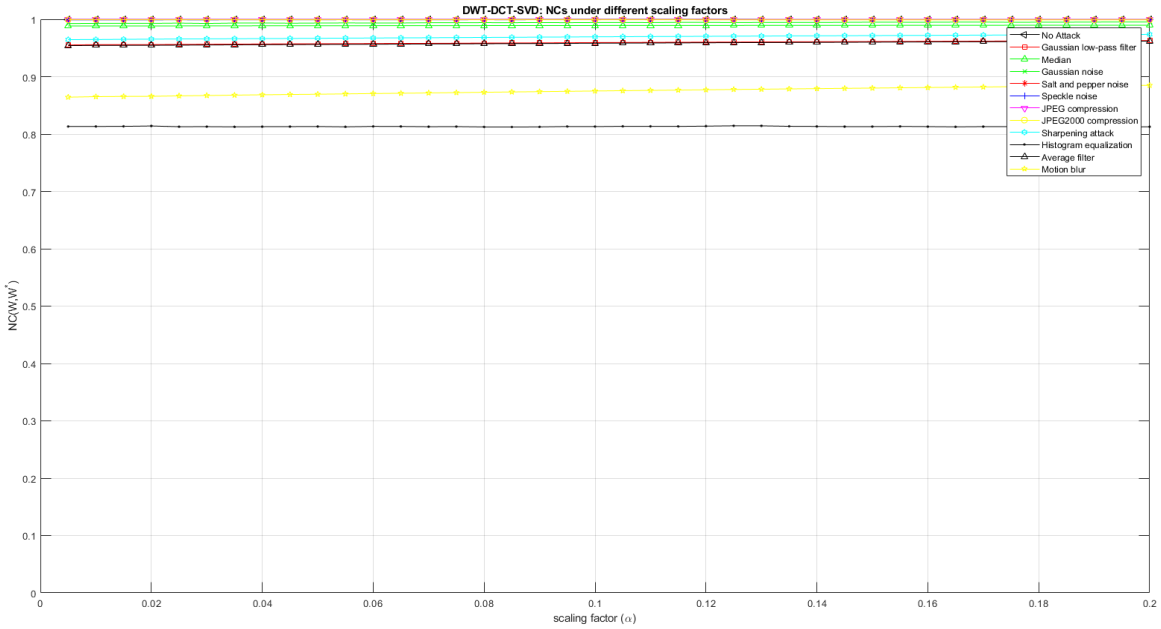

Fig 15 Scaling factor α vs NC.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

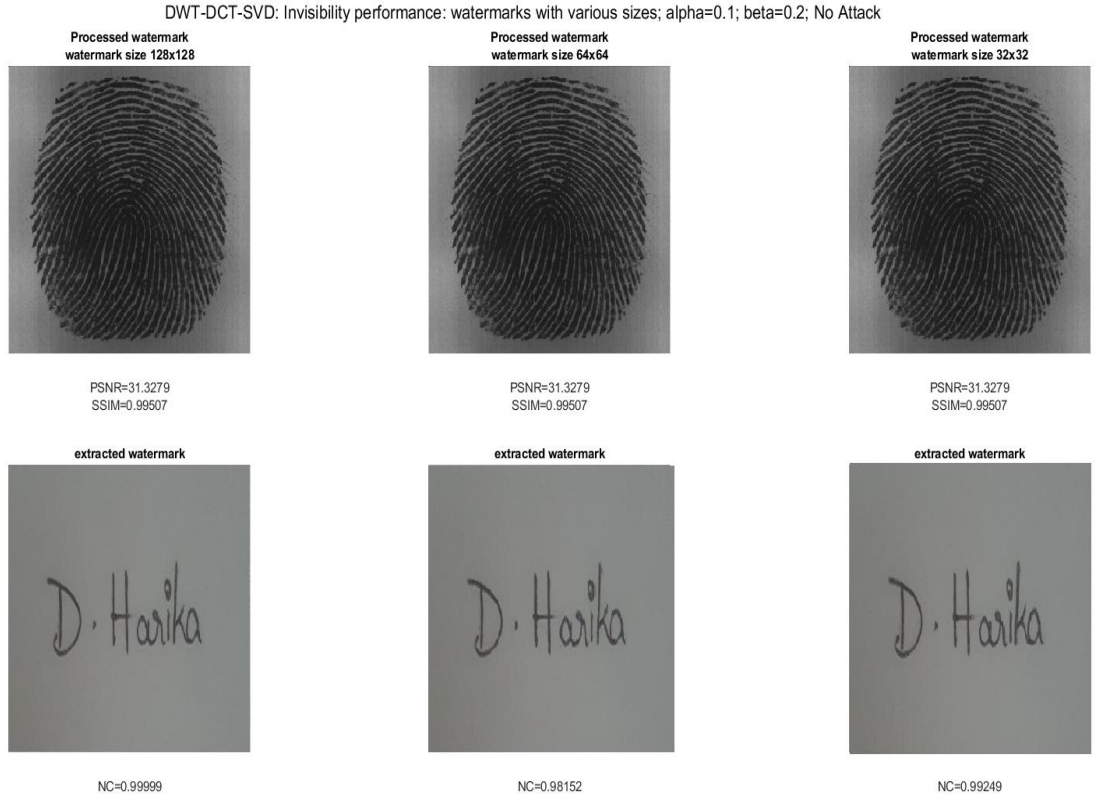

Fig 16 Invisibility performance for α=0.1 with no attack.

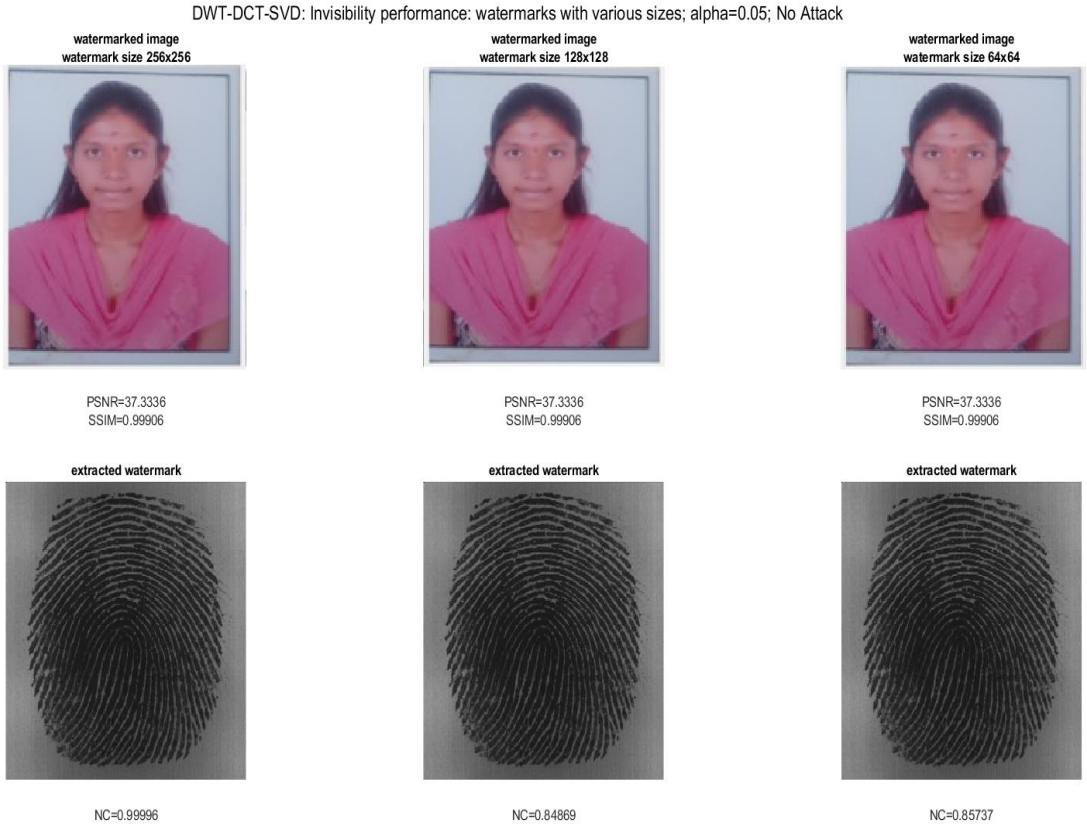

Fig 17 Invisibility performance for α=0.05 with no attack.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

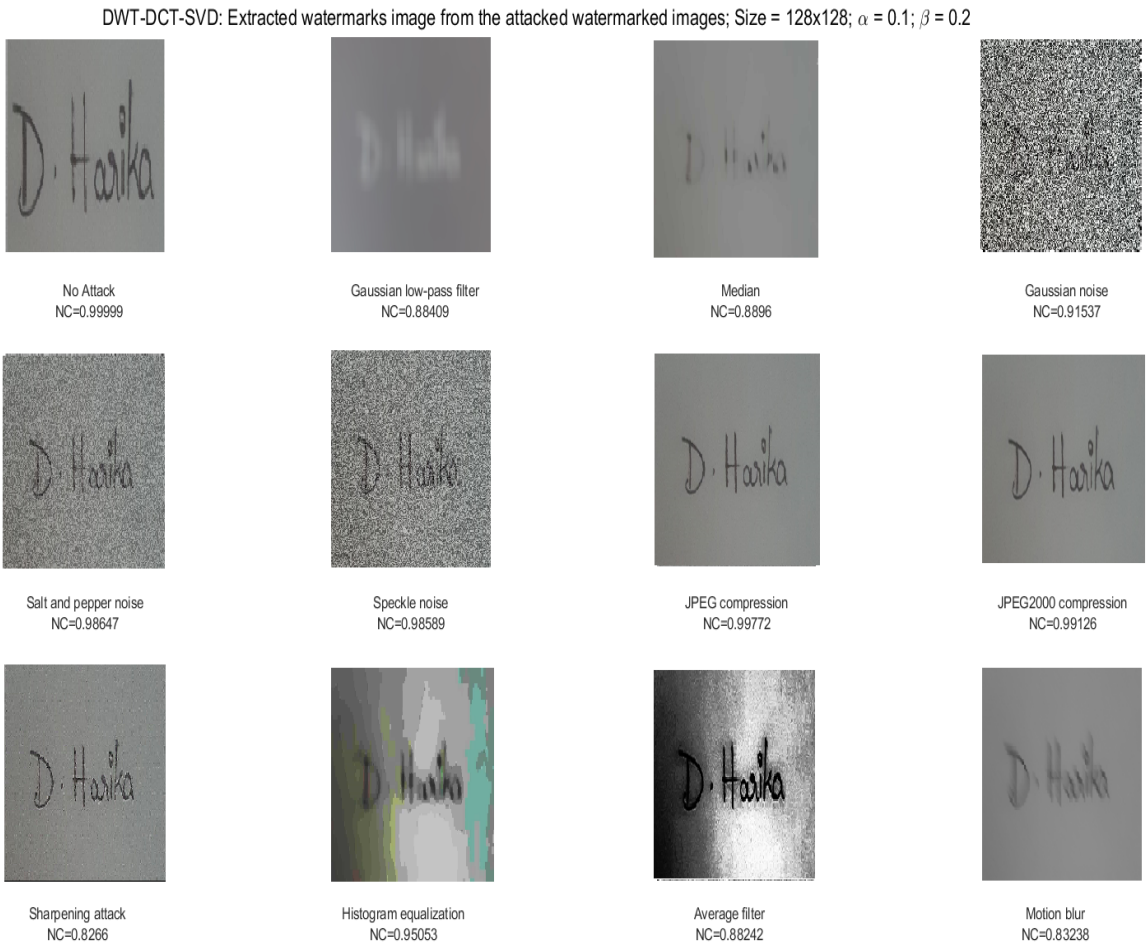

Fig 18 Extracted Watermarked images of size 128x128.

Fig 19 Extracted Watermarked images of size 64x64.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

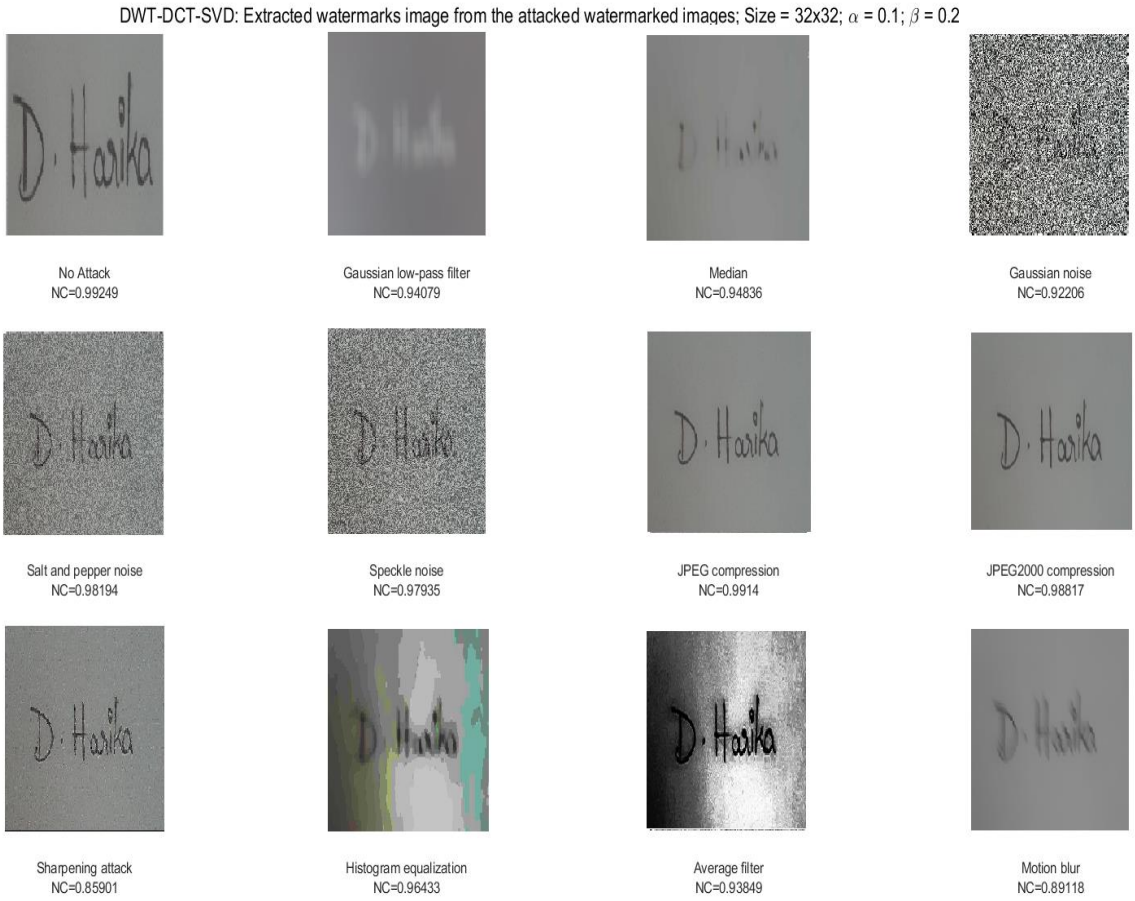

Fig 20 Extracted Watermarked images of size 32x32.

Fig 21 DWT-DCT-SVD method with α=0.1 and no attack.

DOI:10.46647/ijetms.2023.v07i01.023 ISSN: 2581-4621

Conclusion

The proposed work extends a scheme of watermarking that is a combination of spatial and transform domain methods. The DWT-DCT-SVD technique to embed watermark can be of the same size as that of cover image due to the shift invariant feature of RDWT. Here in the proposed method the outcome of RDWT implementation of watermarked images has high PSNR and Normal Cross Correlation. The results illustrate, suggested method is not only efficient in defending against attacks but also improving the performance with respect to noise. In the course of time, a new plan to upgrade the strategy of watermark embedding considering the loopholes. In the future, this work can be extended for video, audio, 3D images and other biometric features like iris, face, voice, palm, etc.

References

1. “Dual Watermarking Technique for Image Authentication using Biometrics”, Bhargavi Mokashi, 978-0-7381-4662-1/21/$31.00 ©2021 IEEE Pg.No 427-432.
2. Ernawan, Ferda, Dhani Ariatmanto, and Ahmad Firdaus. "An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients." *IEEE Access* 9 (2021): 45474-45485.
3. Kahlessenane, Fares, et al. "A DWT based watermarking approach for medical image protection." *Journal of Ambient Intelligence and Humanized Computing* 12.2 (2021): 2931-2938.
4. Zainol, Zurinahni, et al. "Hybrid SVD-based image watermarking schemes: a review." *IEEE Access* 9 (2021): 32931-32968.
5. Begum, Mahbuba, Jannatul Ferdush, and Mohammad Shorif Uddin. "A Hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition." *Journal of King Saud University-Computer and Information Sciences* (2021).
6. Alzahrani, Ali, and Nisar Ahmed Memon. "Blind and Robust Watermarking Scheme in Hybrid Domain for Copyright Protection of Medical Images." *IEEE Access* 9 (2021): 113714-113734.
7. Alzahrani, Ali. "Enhanced Invisibility and Robustness of Digital Image Watermarking Based on DWT-SVD." *Applied Bionics and Biomechanics* 2022 (2022).
8. Zeebaree, Diyar Q. "Robust watermarking scheme based LWT and SVD using artificial bee colony optimization." *Indonesian Journal of Electrical Engineering and Computer Science* 21.2 (2021): 1218-1229.
9. Rajani, D., and P. Rajesh Kumar. "An optimized hybrid algorithm for blind watermarking scheme using singular value decomposition in RDWT-DCT domain." *Journal of Applied Security Research* 17.1 (2022): 103-122.
10. Ikbal, Febina, and R. Gopikakumari. "Performance analysis of SMRT-based color image watermarking in different color spaces." *Information Security Journal: A Global Perspective* (2021): 1-11.
11. Kumar, Parmalik, and A. Sharma. "A robust image watermarking technique using feature optimization and cascaded neural network." *International journal of computer science and information security (IJCSIS)* 18.8 (2019).
12. Fares, K., Amine, K., & Salah, E. (2020). A robust blind color image watermarking based on Fourier transform domain. Optik, 208, 164562.
13. Liu, J., Huang, J., Luo, Y., Cao, L., Yang, S., Wei, D., & Zhou, R. (2019). An optimized image watermarking method based on HD and SVD in DWT domain. IEEE Access, 7, 80849-80860.
14. He, Y., & Hu, Y. (2018, May). A proposed digital image watermarking based on DWT-DCT-SVD. In 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC) (pp. 1214-1218). IEEE.
15. Arora, H., Bansal, C., & Dagar, S. (2018, October). Comparative study of image steganography techniques. In 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) (pp. 982-985). IEEE.
16. Singh, D., & Singh, S. K. (2017). DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. Multimedia Tools and Applications, 76(11), 13001-13024.