Impact in the performance measures for watermark Specific embedding on a hybrid digital image watermarking framework

Saharul Alom Barlaskar[1,a], Anish Monsley Kirupakaran[1], Ashfaq Hussain[1], Masuma Aktar[1], Rabul Hussain Laskar[1] and Taimoor Khan[1]

[1]Department of ECE, National Institute of Technology Silchar, Cachar 788010, Assam, India
[a]*saharul_rs@ece.nits.ac.in*

Abstract. This paper presents an analytical study on the watermark specific embedding in the hybrid digital watermarking framework. Watermark is inserted in the modifications of singular values of SVD domain. To maximize the image imperceptibility and robustness of extraction with adequate security, three important study have been presented in this paper. The excellent re-constructional features of integer wavelet transform (IWT) have been integrated with DCT-SVD domain to obtain adequate visual quality of the watermarked image. The hybrid DCT-SVD features are proved to be sufficiently flexible in the image processing attacks condition. Impact of text image as watermark in the performance parameters have been presented and compared with other general image as watermark. SVD side matrix as a key information at the recipient end helps to avoid the rising FPP problem in SVD domain. The performance of the system have been judged in presence of various image processing attacks, in terms of parameters such as PSNR, NCC, BER, SSIM, and NSR values. The experimental results and analysis validates the scheme is sufficiently flexible to tackle attacks, and exhibits adequate imperceptibility and robustness.

Keywords: *Imperceptibility, robustness, Singular-value- decomposition, integer wavlet transform.*

1. Introduction

The increase in popularity of internet technology to the common user has led to widening of digital multi-media application in day-today life. Copyright protection of multi-media data has become a serious concern in the recent decades. The loss of privacy in digital content has affected severely in many digital data application. In order to protect the copyright of the legitimate user, researcher adopted digital watermarking [4, 5, 11] is one of the viable solution other than steganography [5], where the watermark is superimposed in the digital data either in spatial or frequency domain. Watermarking in frequency domain provides sufficient flexibility of payload as well as robustness compared to spatial domain as seen in many literature [1, 6, 14]. In general, visible and invisible are two perceptual property of watermark that exists in watermarking technology [9]. In the perspective of security, invisible property of watermark has gained much attention compared to its counterpart [10]. The technique which utilizes detection method without any input information from the sender end is termed as blind detection, whereas certain reference input is required in case of non-blind kind of watermark [17]. Robustness, image imperceptibility, and payload or

R. Murugan et al. (eds.), *Proceedings of the International Conference on Signal Processing and Computer Vision (SIPCOV 2023)*, Advances in Engineering Research 239,
https://doi.org/10.2991/978-94-6463-529-4_9

capacity are three important features of a typical watermarking system which in combined governs the system performance [9, 10]. There also exists a conflicting relationship amongst the three parameters. Apart from these parameter sets, the security of watermark need to ensure for successful delivery of the digital content to the legitimate user. Normalized correlation coefficient (NCC) is used to determine the robustness of detected watermark. Image imperceptibility is evaluated by computing peak-signal-to-noise-ratio (PSNR) between host and watermarked image. Other parameters [6, 10] such as NSR (normalized similarity ratio), and structural similarity index measure (SSIM), bit error rate (BER) are also governs the quality of watermark extraction.

2. RELATED WORK

Although the process of modification or insertion of watermark in spatial domain provides flexibility in terms of capacity [3,7], but the technique performs poorly under image processing attack conditions. Many transform domain such discrete-cosine-transform, Fourier transform, and other wavelet based transformation method have been used in many literature [8, 15] to increase the robustness under image processing attack condition. As, DFT fails to give location information which is substituted by its counterpart DWT [1, 3, 4] in data hiding application. The attractive multi-resolution capability incorporating human visual perception modelling by the DWT coefficient has attained significant attention in the watermarking application [9]. However, failing of directional property is the bottleneck of DWT based framework as revealed in [2].

At the same time, other wavelet such as Lifted-wavelet-transform possess less computational requirement with minimum memory, stationery-wavelet-transform which also exhibits fast computational speed, counterlet transform, etc., are the dominant transformation technique used in watermarking techniques [2,11, 12]. Thus the literature study suggests every domain exhibits its unique inherent resiliency property which is helpful to improve system performance.

Many hybrid technique are also available recently in literature [12, 13,18] which shows the systems are capable of providing sufficient robustness and image visual quality of the watermarked image. However achieving adequate capacity is scarce minimum at the same time due to conflicting nature. The major advantages of such technique is to utilize the dual benefits of individual domain, where weakness of one domain is waived out by the other. In [13, 19], DWT is seen to use in combine with DCT. Although the excellent energy compaction property of DCT is helpful to certain compression kind of attack, however DCT does not support HVS and which is overcome by DWT. Moreover, wavelet decomposition segregate the images in to different frequency bands, which is not necessarily an optimal representation of the image. So, singular value decomposition (SVD) method is being explored.

Singular value decomposition method is the most powerful tool used in mathematics to analyze rectangular matrices [4]. The singular value component of SVD method shows a good stability factor and doesn’t changes even under minor attack condition and as a result it was used extensively in earlier steganography application. SVD also shows good proportion and rotation invariance property [4]. This property makes it a suitable option in watermarking application to guarantees robustness under attacks condition.

Most of the watermarking scheme used grayscale image as a host to embed watermark. Also, it is seen researcher used mainly text images as watermark in [10]. The advantages of embedding text images provides sufficient reliability to reconstruct during detection phase adopting extensive transform features, also easy of designing extracting algorithm. Moreover, there is still lack of study left to extract both generic image as well as text image as watermark in particular watermarking scheme. This study has been incorporated in this proposed work to understand the flexibility to detect watermark under the proposed watermarking framework.

The major drawback of DWT based scheme is the lack of accurate data reconstruction due to truncation loss during reverse transformation of images. The features of integer to integer transform exhibited by integer wavelet transform has made it an attractive choices in the accurate data recovery process. As a result, IWT is an emergent technique after the DWT. The hybrid combination of IWT-DCT-SVD has been utilized in this proposed work to achieve better robustness, image imperceptibility, and the maximum capacity of watermark.

The paper is arranged as follows: preliminaries about IWT, DCT, and SVD. Section 2, Section 3 discuss about the watermark insertion, extraction which are followed by discussion of results, and conclusion.

3. PRELIMINERIES

3.1. Integer Wavelet Transform

Swelden's [2] introduced the integer wavelet transform as a countermeasure of the limitations of the conventional DWT. DWT considers the input as a floating point values but in practice image is represented as integer values in image processing. As a result, there is truncation loss appears during reconstruction time, whereas the integer to integer mapping in IWT eliminates this truncation loss completely, which is a primary requirement to preserve image visual quality knows as imperceptibility. Lifted scheme [1, 2] demonstrated (in Fig.1) offers less memory requirement, and light computational necessity. So, IWT utilizes this lifted scheme, as this process is a reversible process. Hence perfect reconstruction is possible.

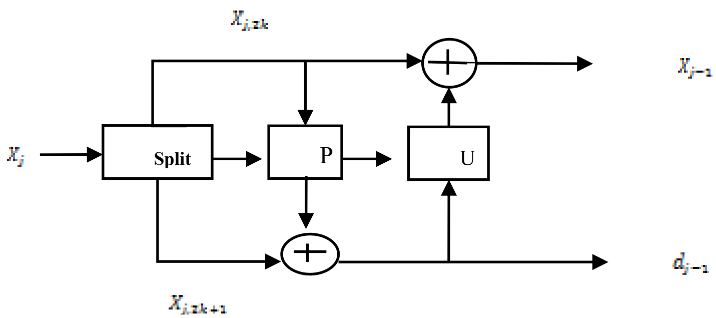


Fig.1: Decomposition using lifted wavelet scheme [2]

3.2 Discrete Cosine transform

DCT separates image in to its equivalent frequency coefficients by modifying frequency components, which is represented as sum of its cosine functions. DCT is a real and orthogonal transform, having excellent energy compaction ability in its coefficients values and possess good de-correlation of data points. For an image $'i(x,y)'$, the DCT transformation is represented as follows [10] in Eq (1).

$$I(P,Q) == \frac{2}{\sqrt{MN}} \delta(P)\delta(Q) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left(i(x,y) \cos\left(\frac{P(2x+1)\pi}{2M}\right) \cos\left(\frac{Q(2y+1)\pi}{2N}\right)\right) \tag{1}$$

Where, $P = 0,1,2, \dots \dots \dots M-1$, $Q = 0,1,2,3 \dots \dots N-1$ and $\delta(P), \delta(Q)$ are constant.

3.3 Singular Value Decomposition

Singular value decomposition is a linear algebra procedure to diagonalizable a rectangular matrices very easily. SVD [7, 15], decomposed a real matrices in to its three equivalent matrices namely U, S, and V respectively, where U, V are two orthogonal matrices and S is the singular metrics. In image processing application, this two orthogonal matrices carry image information, and the singular value carries intensity of the images. The diagonal singular values are arranged in decreasing order. If λ_1, λ_2, λ_3, $\lambda_4 \dots \lambda_M$ are the singular values of M×N matrices, then the arrangement of diagonal values follows the pattern as $\lambda_1 > \lambda_2 > \lambda_3 > \lambda_4 \dots > \lambda_M$.

4. Watermarking in hybrid IWT-DCT-SVD domain

The proposed watermarking technique embeds grayscale watermark image of size (256×256) in to a covert image (512×512). IWT has been used to achieve 1-level decomposition of the covert image as shown in Fig.2. The process of embedding and extraction of watermark is illustrated in Fig.3. The HL sub-band have been utilized for watermark insertion purpose. As this sub-band carries horizontal details of the images, and mostly carries uniform frequency information in its transform coefficients so the possibility of the changes has minimal affect in this frequency band. Moreover, sub-band such as HH, carries high frequency edge and texture information, and most of the energy of natural images concentrated in LL sub band. So, modification in such sub-band may cause severe visual affect. So DCT have been performed to the transform sub-band to get equivalent DCT coefficients values, followed by SVD operation is carried out on these DCT coefficients 'F_{DCT}' to get U, S and V matrices.

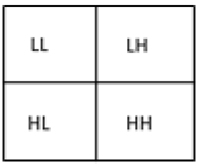


Fig.2: 1-Level IWT decomposition

The major drawback of SVD based system is the rise of false positive detection at the receiver end due to presence of its two side matrices such as U and V in SVD decomposition. The sender needs to share the U, V matrices to extract watermark and as a result it creates an ambiguity during detection phase. So, this FPP problem has been tried to eliminate by incorporating a secret key 'K' which carries one of the decomposed orthogonal matrices of the watermark image 'u_w' in addition to the singular value matrices 's_w'. Thus the modification or embedding of watermark have been achieved by the following Eq (2)

$$S_\theta^n = S_\theta + \varphi(u_w \times s_w) \qquad [2]$$

Here, S_θ is the singular value of the decomposed covert image, φ acts as a scale factor, u_w, s_w are respective orthogonal and singular matrices of the watermark image.

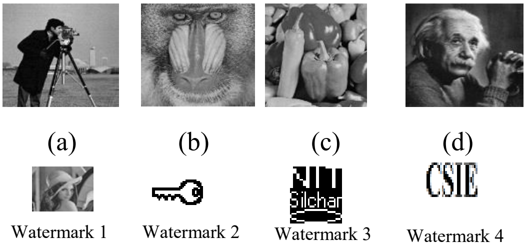


Fig.3 shows standard image used as host (a) Cameraman, (b) Mandrill, (c) Vegetable, (d) Einstein and other different watermark image version

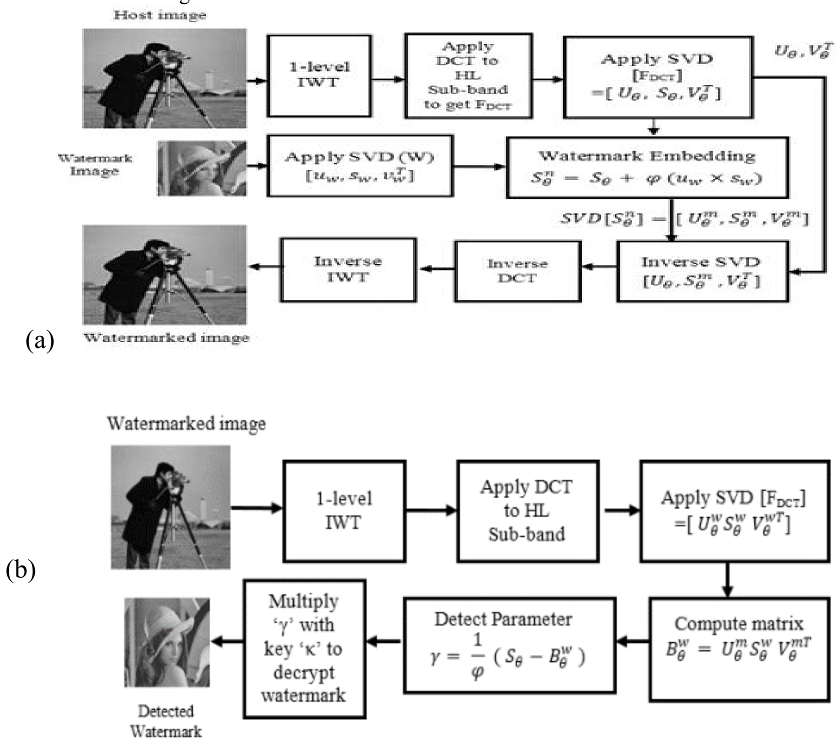


Fig.4: Illustrates system architecture (a) watermark embedding process, (b) watermark extraction process.

Thus, the extraction of watermark involves sharing of dedicated secret key (K) which provides a completely free to extract watermark, free from false positivity as occurs in conventional method. So, the method provides security to protect the copyright perspective to the genuine user. At the same time, utilizing hybrid features of IWT-DCT-SVD enables sufficient resiliency in robustness, image visual quality with adequate watermark capacity of embedding.

5. RESULTS AND DISCUSSION

In this section, the experimental result of the proposed method is presented. Our system is implemented in MATLAB 2019a, equipped with a system facility of Intel(R) Xeon(R) Gold 6254 CPU, 128 GB RAM. A standard host image 'Cameraman' of size (512×512) is used for embedding watermark of size (256×256). While doing the experimentation different other watermark images (such as text image, general images) were also used to see the system flexibility in presence of various image processing attacks. The performance of the system have been evaluated in terms of standard performance measuring parameters. Image quality of watermarked image have been evaluated by measuring peak-signal-to-noise ratio between two images and is represented by the Eq.3.

$$PSNR = \log_{10}\left[\frac{512 \times 512 \times \max\ [I(p,q)^2]}{\sum_{p=1}^{512}\sum_{q=1}^{512}[I(p,q) - I'(p,q)]^2}\right] \quad (3)$$

Here, $I(p,q)$ and $I'(p,q)$ are covert and watermarked images, PSNR is measured in dB. Normalizes correlation coefficient (NCC) have been used to judge the robustness values between original and extracted watermark.

$$NCC = \frac{\sum_{i=1}^{256}\sum_{1}^{256} W(i,j) \times W_{W}(i,j)}{\sum_{i=1}^{256}\sum_{1}^{256} W(i,j) \times W(i,j)} \quad (4)$$

And the normalized similarity ratio (NSR) is computed by using Eq. (5)

$$NSR = \frac{SR - \min(SR)}{1 - \min(SR)} \quad (5)$$

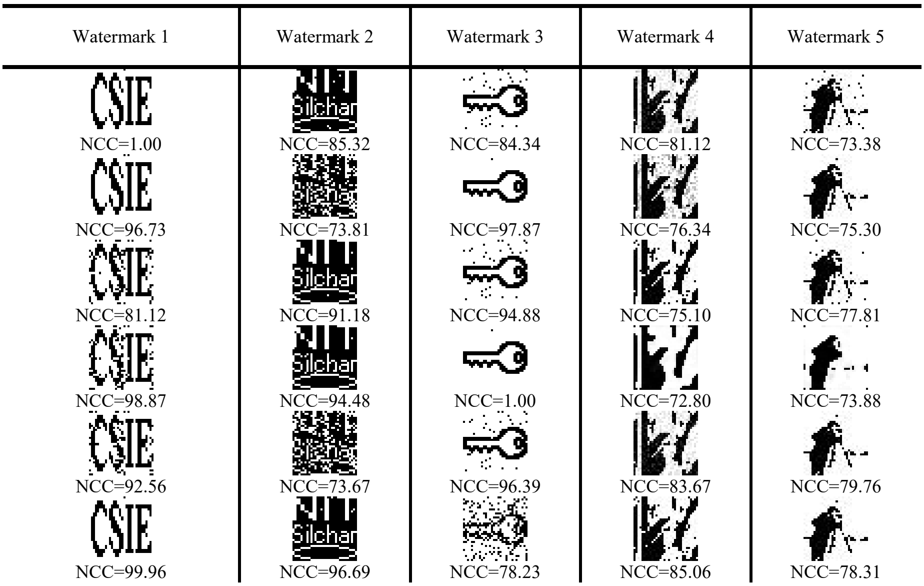
Where NSR [18] is depends on the similarity ratio, which given by

$$SR = \frac{S}{S + C} \quad (6)$$

Where S is the total number of similar pixels in original watermark and C is the total number of corrupted image pixels in the extracted watermark. Instead of using conventional error summation method to compute distortion, SSIM is derived by modelling three different image distortion factors such as loss of correlation, luminance distortion, and contrast distortion [11, 17]. There are mainly three sets of experiment have been carried out to present the performance of hybrid IWT-DCT-SVD based watermarking scheme. Firstly, different watermark images were tested on the system to know the watermark specific robustness in presence of image processing attacks. Secondly, robustness of the system have been judged in particular in presence of varying degree of noise attack. This study gives a generic robustness performance under attack conditions. At the last, watermark specific effect on the visual quality of watermarked image have been presented.

Experiment-I: Robustness study under influence image processing attacks.

Initially, an experiment have been performed to embed watermark of capacity (256×256) in the modifications of singular values as demonstrated in the embedding stage. A standard image such as 'cameraman' (shown in Fig.4), have been chosen as host to embed watermark. In order to understand the robustness variation in presence of various attack. Distinct watermark images such as text image, logo images, and general images (shown in Fig.3) were considered to judge the resiliency during attack condition. The varying nature of watermark quality indicates that every watermark itself possess resiliency against attacks, and which also helps to retain watermark robustness. The amount of information from image to image varies due to presence of quantity of image information. Thus, a usual text image always carries less energy compared to general logo images. This study have been made particularly to see the impact on robustness during attack conditions for embedding of distinct sets of watermark image. So, five different watermark have been selected to perform the experiment and have been marked as 'watermark 1',' watermark 2',' watermark 3',' watermark 4',' watermark 5'. Few image processing attacks with varying density of noises such as salt-and-pepper noise (SN) [0.02%, 0.05%] , Gaussian noise (GN) [0.02%], impulse noise (IN), speckle noise (SPN), histogram equalization (HE), gamma correction (GC) have been applied on the watermarked image (cameraman). The embedding and extraction of watermarks are done by fixing a scale factor (γ=0.05) value. Fig.3 shows various extracted watermark images under attack conditions. From the results, it is clear the extracted marks are found to show good robustness (NCC) percentage (above 75%) in most of the cases. However, the variation of NCC have been significantly higher for the textual images compared to general logo images. As the text image carries less information, the influence of attack is minimum on the watermark coefficients. The SVD features are sufficiently flexible to withstand the impact. As a result, the robustness (NCC) is gets possibly boosted up.



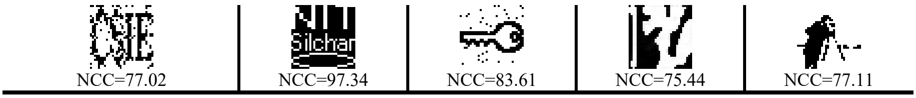


Fig.5: Robustness (NCC) for distinct watermark images

Experiment-II: Variation of robustness due to embedding of distinct watermark images

To understand the system robustness, an experiment have been carried out imposing various signal processing attack with varying degree of noise. A standard image 'cameraman' have been used as for watermarking purpose, and sets of different noises applied on it before extracting watermark. Various performance measures such as normalized correlation coefficient (NCC), structural similarity index measures (SSIM), normalized similarity ratio (NSR), and bit error rate (BER) computed for the extracted watermark image. The robustness performance have been presented in Table.1. The results depicts clearly there is a consistent of robustness even though variations of noise density. The use of hybrid features enable to retain both robustness and other structural identity excellent manner.

The excellent DCT features combine with SVD stability property plays a significant role to sustain robustness of watermark during image processing attack condition. The extracted watermark almost resembles to its original watermark in most of the attack condition as it is clearly visible in the Fig.3. So, this study validates that there is sufficient resiliency can be achieved under attack condition in the hybrid scheme compared to the state-of-art available technique with least effort.

Table 1*: Robustness (NCC) of watermark under different attack condition.*

Attacks	NCC	SSIM	NSR	BER
Salt & pepper (0.01%)	0.9891	0.9899	0.9898	0.0103
Salt & pepper (0.02%)	0.9794	0.9907	0.9955	0.0136
Salt & pepper (0.03%)	0.9857	0.9997	0.9988	0.0044
Poisson noise	0.7738	0.9914	0.9774	0.0257
Speckle noise (0.001)	0.8957	0.9814	0.9789	0.0354
Speckle noise (0.005)	0.8704	0.9484	0.9476	0.0470
Speckle noise (0.009)	0.8566	0.9546	0.9895	0.0318
Gaussian noise (0.001)	0.9862	0.9970	0.9998	0.0068
Gaussian noise (0.005)	0.9532	0.9996	0.9897	0.0341
Gaussian noise (0.009)	0.9423	0.9766	0.9101	0.0541
Cropping (Top-Left)	0.9414	0.9476	0.9879	0.0029
Cropping (Bottom-Right)	0.9748	0.9877	0.9839	0.0151
Scaling (0.9)	0.9668	0.9898	0.9870	0.0116
Rotation (5 degree)	0.9830	0.9821	0.9749	0.0054
Gamma correction	0.9897	0.9903	0.9993	0.0037
JPG (Q = 90)	0.9543	0.9981	0.9993	0.0156
JPG (Q = 90)	0.9830	0.9970	0.9989	0.0058
JPG (Q = 85)	0.9943	0.9905	0.9769	0.0019
Gaussian filter (3 × 3)	0.9831	0.9999	0.9869	0.0056
Average filter (3 × 3)	0.9641	0.9971	0.9478	0.0048

Median filter (3 × 3)	0.9970	0.9998	0.9748	0.0110
Histogram Equalization	0.9532	0.9897	0.9876	0.0181

Experiment-III: Influence on imperceptibility due to distinct watermark images. Imperceptibility, is a term gives a measure of image perceptual quality when the image content is made change [9, 13, 16]. A watermarking scheme is considered as an efficient when this perceptual degradation is least to user perception. So, in order to understand the imperceptibility factor four different host images were watermarked individually with five different watermark images. The watermarking effect have been presented in the bar graph as shown in Fig.6. A particular image showing different PSNR indicates the variations of image quality due to distinct watermarking effect. The results demonstrates there is good PSNR possible due to embedding of watermark 1 and watermark 2, which means that these image corresponds to text images as watermark. Since the text image carries less information compared to other general image and are not sensitive to Information loss, as a result the possibility of image degradation is least which helps to improve image imperceptibility factor. Thus, the study proved that text image as watermark performs better compared to general image in the hybrid framework.

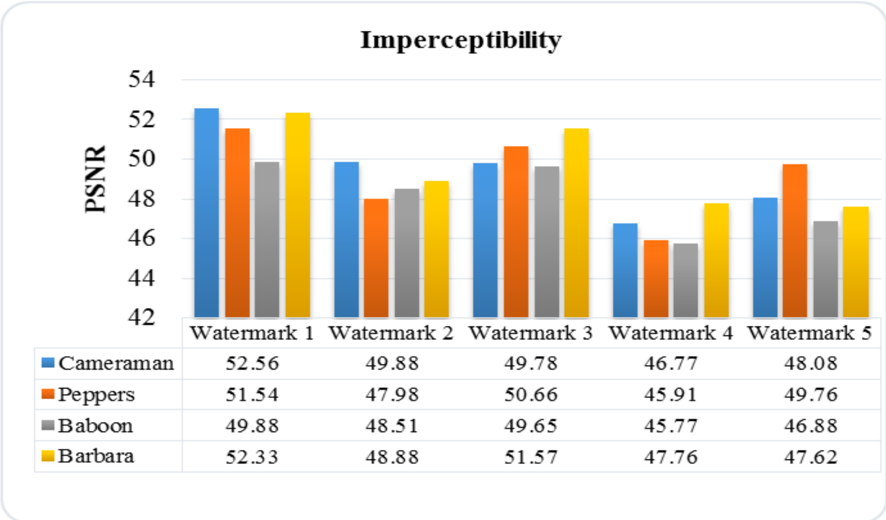


Fig.6 Imperceptibility (PSNR) variation for different standard images.

6.Conclusion

A detail study on image imperceptibility and robustness have been presented with experimental results for the proposed hybrid IWT-DCT-SVD method of watermarking. The incorporation of integer based wavelet facilitates a good visual quality in terms of PSNR (above 45 dB) irrespective of the type of watermark used. The replacement of conventional wavelet by integer wavelet transform is a good choices which overcomes many limitations of its counterpart. The technique provides average PSNR~48dB in case of standard cameraman image which is an acceptable choice (visual quality) in the diverse attack condition. The advantages of hybrid features helps to provide sufficiently flexible robustness even at varying density of noise condition. Thus, the proposed results suggest that the technique is suitable for copy right protection of digital data. Further as an extension of this work, other sub-band and enhancement of capacity may be considered for future level of study. Additionally, the work may be extended to implement for color images also.

ACKNOWLEDGMENT

The author would thank the members of speech and image processing laboratory for all their support to carry this research work.

References

[1] F. Yasmeen, M.S. Uddin, An Efficient Watermarking Approach Based on LL and HH Edges of DWT SVD, SN Comput. Sci. 2 (2021) 1–16. https://doi.org/10.1007/s42979-021-00478-y.

[2] Swelden's, W.: The lifting scheme: a construction of second generation wavelets. SIAM journal on mathematical analysis **29**(2), 511–546 (1998) 10. Khayam, Syed Ali. "The discrete cosine transform (DCT): theory and application." Michigan State University 114, no. 1 (2003):31

[3] K. Loukhaoukha, J.Y. Chouinard, M.H. 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.

[4] M. Ali, C.W. Ahn, M. Pant, A robust image watermarking technique using SVD and differential evolution in DCT domain, Optik (Stuttg). 125 (2014) 428–434. https://doi.org/10.1016/j.ijleo.2013.06.082.

[5] V.S. Verma, R.K. Jha, An Overview of Robust Digital Image Watermarking, IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India). 32 (2015) 479–496. https://doi.org/10.1080/02564602.2015.1042927.

[6] Punidha, R. Sivaram, M.: Integer Wavelet Transform Based Approach for High Robustness of Audio Signal Transmission. Int. J. Pure Appl. Math. 116, 295–304 (2017)

[7] Makbol, N. M., Khoo, B. E.: A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition', Digital Signal Processing, vol. 33, pp. 134-147.

[8] Thakkar, F., Srivastava, V.K.: An adaptive, secure and imperceptive image watermarking using swarm intelligence, Arnold transform, SVD and DWT. Multimed. Tools Appl. 80, 12275–12292 (2021). https://doi.org/10.1007/s11042-020-10220-0

[9] Islam, M., Laskar, R.H.: Robust image watermarking technique using support vector regression for blind geometric distortion correction in lifting wavelet transform and singular value decomposition domain. J. Electron. Imaging. 27, 1 (2018). https://doi.org/10.1117/1.jei.27.5.053008

[10] S.A. Barlaskar, S.V. Singh, A.M. Kirupakaran, and R.H. Laskar. "Genetic algorithm based optimized watermarking technique using hybrid DCNN-SVR and statistical approach for watermark extraction." Multimedia Tools and Applications, Vol. 81, no. 5, pp. 7461-7500, 2018.

[11] G. Bhatnagar, and Q. J. Wu, "A new logo watermarking based on redundant fractional wavelet transform, "Mathematical and Computer Modelling. 2013 Jul 31; 58 (1):204-18.

[12] Salama, Ahmed S., and Mohamed Amr Mokhtar. "Combined technique for improving digital image watermarking." In *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, pp. 557-562. IEEE, 2016.

[13] D. Singh and K. S. Singh. "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection." *Multimedia Tools and Applications* 76, no. 11 pp. 13001-13024, 2017.

[14] A.K. Singh, "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images." Multimedia Tools and Applications, Vol. 76, no. 6, pp. 8881-8900, 2017.

[15] S. Bagheri Baba Ahmadi, G. Zhang, S. Wei, L. Boukela, An intelligent and blind image watermarking scheme based on hybrid SVD transforms using human visual system characteristics, Vis. Comput. 37 (2021) 385–409. https://doi.org/10.1007/s00371-020-01808-6
[16] C. Kumar, A. K. Singh, and P. Kumar. "A recent survey on image watermarking techniques and its application in e-governance." Multimedia Tools and Applications, Vol. 77, no. 3 (2018): 3597-3622.
[17] Lee, Chin-Feng, Jau-Ji Shen, and Zhao-Ru Chen. "A survey of watermarking-based authentication for digital image." In *2018 3rd International Conference on Computer and Communication Systems (ICCCS)*, pp. 207-211. IEEE, 2018.
[18] Singh, Durgesh, and Sanjay K. Singh. "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection." *Multimedia Tools and Applications* 76, no. 11 (2017): 13001-13024.
[19] Islam, M., G. Mallikharjunudu, A. S. Parmar, A. Kumar, and R. H. Laskar. "SVM regression based robust image watermarking technique in joint DWT-DCT domain." In 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), pp. 1426-1433. IEEE, 2017.