Journal of Engineering and Applied Sciences 14 (23): 8712-8720, 2019
ISSN: 1816-949X

Evaluating the Robustness of Image Watermarking System based on Multilevel Wavelet Transform

[1]Heyam Maraha, [2]Kameran Ali Ameen, [1]Dalya Raad Abbas, [3]Raghad Zuahir Yousif,
[1]Ahmed M. Fakhrudeen and [2]Aras Al-Dawoodi
[1]Department of Network,
[2]Department of Computer Science, College of Computer Science and Information Technology,
Kirkuk University, Kirkuk, Iraq
[3]Department of Applied Physics and Communication, College of Science, Salahuddin University,
Erbil, Kurdistan Region, Iraq

Abstract: Scheme of "robust image watermarking" for the protection of copyright is proposed based on "3-level 2-Dimensional Discrete Wavelet levels decompositions (2DDWT)". In the proposed system, two binary watermark images are embedded into the sub-bands of a cover image by using direct arithmetic addition depending on the alpha blending with variable scaling factor scheme with the host image wavelet coefficients. A comparison has been made among 1-3 level through the use of statistical parameters like "Peak-Signal-to-Noise-Ratio (PSNR)" and Similarity Ratio (SR). Then five groups of malicious attacks are applied to watermarked images like filters, noises, geometric, JPEG compression and restoration and enhancement attacks on the watermarked image which is the main contribution to this field. The experimental results show that the watermark images generated with the proposed algorithm based on 3-levels outperform the other levels in terms of robustness. However, they show comparable results in terms of transparency. As a result, the 3rd level is recommended for watermarking schemes.

Key words: 2DDWT, watermarking, PSNR, SR, embedding, extraction

INTRODUCTION

On account of the rapid advancement multimedia technology and popularity of the internet, the use of protecting intellectual property rights technique has become an urgent issue to prevent unauthorized people steal or alter the host media through the internet. Digital watermarking has attracted considerable attention to conserving intellectual property rights from unauthorized people (Lai and Tsai, 2010). The digital watermark refers to the signal that is embedded permanently into digital data (text, images, audio and video). Later, computing operations can be used to detect or extract this signal, so that, the data would be asserted. The host data hide the watermark in a way that it can be separated from the data and so that, it is resistant to many operations not degrading the host document (Gupta, 2012).

Watermarking can be categorized as visible or invisible. A visible watermarking example is the logo visible overlie on the corner of a television channel in a television scene. On the other hand, the invisible watermark is hidden in the object which can be detected by an authorized person. Invisible watermark is branched out into two types:

- Invisible-robust watermark
- Invisible-fragile watermark (Thapa *et al*., 2011)

There are several digital watermarking applications that could be summarized as:

- Copyright protection
- Broadcast monitoring
- Tamper detection
- Authentication and integrity verification
- Fingerprinting
- Content description
- Covert communication (Podilchuk and Delp, 2001)

Figure 1 shows the general system of watermarking. Embedding, transmission and extraction are the three stages of the watermarking system. In the first stage

Corresponding Author: Heyam Maraha, Department of Network, College of Computer Science and Information Technology, Kirkuk University, Kirkuk, Iraq

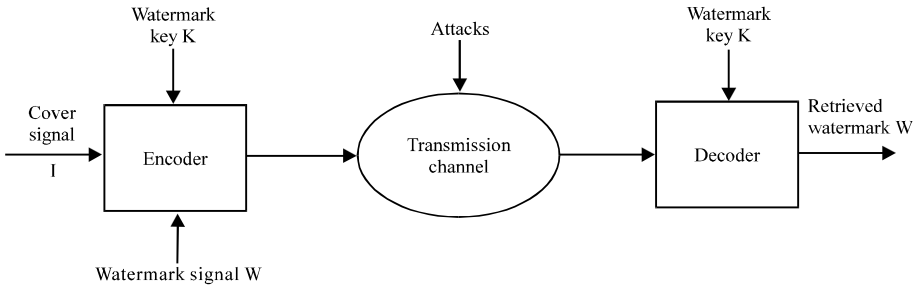

Fig. 1: Digital watermarking system

known as embedding, a specific key is used to encode the watermark in the cover data. For an additional level of protection, the watermark is encrypted using this particular key. This may ensure that the media can be extracted only by an authorized media player. Concerning signature, it represents the watermark signal which would be embedded in the copyright media. The embedding process has resulted in the watermarked image. Then, this image is transmitted to the recipient. The watermarked image in the process of transmission might be exposed to attacks. These attacks occur either intentionally or because of error in transmission or noise. Nonetheless, the decoding of data is required for extracting the watermarked image (Song *et al*., 2010).

The digital watermarking system depicted in Fig. 1 is defined by these parameters (I, I', K, W) where, I represents the cover image, I' denotes watermarked image while K represents the secret key and W denotes the watermark signal.

Watermarking techniques could be classified into different categories according to several criteria. Depending on the domain criteria, there are two techniques: the spatial and transform domain. The first one deals with pixels itself without transformation like (LSB) while the second one transforms the original media into the frequency domain using different types of frequency transformation algorithms like (DCT, DWT, DFT). Encoding of the spatial domain is relatively less useful than the transformed watermarking (Ram, 2013). There are three classes of watermarking technologies which are based on the information available for the extraction and detection processes. The first class is called blind watermarking technique which needs at least the host signal I in the detection process for the watermark. The second class is named semi-blind watermarking technique. In this class, in order to detect the watermark, the system doesn't require I but may need any of the following parameters (I', K, W). On the other hand, the third class known as non-blind watermarking technique is the most difficult one because it needs neither the original signal I nor the watermark signal W but may need these parameters (I', K, W') (Maraha, 2014; Kashyap and Sinha, 2012).

An efficient watermark should satisfy some essential requirements. The most important elements are in the first place transparency which is the most significant requirement in the watermarking system and it refers to the perceptual similarity between the original image before the watermarking process and the watermarked signal. In the second place the robustness which is the ability to extract or detect the watermark after exposure to hostile attacks. While in the third place, security which ensures that the embedded watermark would not be removed or modified without causing damage to the original signal. The strength of this property depends on the proposed embedding algorithm. Finally, capacity denotes to the amount of information to be embedded in the original media. There must be a trade off between capacity and other features like robustness and transparency because any increase in the capacity size will reduce the effectiveness of these two features (Abdullatif *et al*., 2013; Makbol and Khoo, 2014).

The frequent use of DWT in "digital image watermarking" is attributed to the superiority of its spatial localization and characteristics of multi-resolution which resemble the theoretical models of the human visual system. Increasing the DWT level would result in more improvements in performance in "DWT-based digital image watermarking algorithms". The cover image has areas that can embed the secret image effectively; therefore, these areas are best identified using DWT (Al-Haj, 2007). The masking effect of the human visual system can be exploited through this property. Hence, the modification of DWT co-efficient modifies only the area that corresponds to that coefficient. In the sub-bands with lower frequency, the image might be damaged by the embedding watermark. This is because these sub-bands, generally, store most of the energy of the image. Yet, it is more robust. Information about the image edge is contained in the high-frequency part; thus, watermarking

is performed using sub-bands with high frequency due to less sensitivity of the human eye to edges changes. In this research, "2-Dimensional Discrete Wavelet Transform (2D-DWT)" has been employed in the embedding and inverse 2D-IDWT in the extraction process. The third decomposition level coefficients are involved in the process of embedding and extraction to enhance the security of the watermarking system. Besides, many measures that were employed to test system performance.

Literature review: Pratibha *et al.* use a digital image watermarking on the basis of "3-level Discrete Wavelet Transform (DWT)" and compare it with "1 and 2 levels DWT". They have used "a multi-bit watermark" which is embedded into a host image sub-band with low frequency through the use of "alpha blending technique". The watermark image is dispersed within the original image in embedding that depends on the scaling factor of "alpha blending technique". The same scaling factor that is used in embedding can be used to extract the watermark. Method performance for varied values of the scaling factor is analyzed and compared with "1 and 2 levels DWT" method in accordance with "Peak-Signal-to-Noise-Ratio (PSNR)" and "Mean Square Error (MSE)".

Makbol and Khoo (2014) propose a technique using the "Integer Wavelet Transform (IWT)" and "Singular Value Decomposition (SVD)". The values of grey image watermark pixels are embedded directly into the singular values of "the 1-level IWT decomposed sub-bands". Due to, the properties of IWT and SVD, the results obtained from the proposed scheme shows effectiveness in terms of robustness and capacity. According to the false positive problems caused by most schemes of "SVD-based watermarking", the proposed system solved that by adopting digital signature into the watermarked image. The proposed signature mechanism is used to generate and embed a digital signature after the embedding watermarks process. The proposed scheme proved its efficiency in security and robustness against various attacks.

Deb *et al.* (2012) have proposed a combination of the technique of "DWT-DCT based digital image watermarking" and "low frequency watermarking" with weighted correction. The desirable properties which are scalability offered from DWT based watermarking techniques and compression offered from DCT based watermarking techniques are used in this combined watermarking scheme. In the proposed framework, the bits of the watermark are inserted into the low frequency of each DCT block of the selected coefficient set of DWT domain. Transparency is improved by using the weighted correction. The extracting procedure reverses the embedding operations without the reference of the original image. Comparing the proposed algorithm with the similar approach by DCT and DWT based approach, the experimental results show that the proposed scheme preserves superior image quality and robustness against various attacks such as cropping, JPEG compression, contrast adjustments, sharping and so on.

Tao and Eskicioglu (2004) generalize an idea that embeds a binary image in all four bands of 1st and 2nd levels of "Discrete Wavelet Transform (DWT) decomposition". This generalization compares the watermark that is embedded at 1st and 2nd levels of decompositions for all bands. They test the suggested algorithm against 15 attacks. When the watermark is embedded in lower frequencies, this reveals its robustness to a set of attacks and when it is embedded in higher frequencies, this explains its robustness to another set of attacks, excepting re-watermarking and collusion attacks. All four bands resulted in identical watermarks. The proposed algorithm proved that first level decomposition is better than 2nd level decomposition due to:

- The increased area for embedding the watermark
- More textured watermarks with better visual quality

Al-Haj (2014) proposed an algorithm of digital audio watermarking that is semi-blind. Two transforms are performed in this algorithm:

- The Discrete Wavelet Transforms (DWT)
- The Singular Value Decomposition (SVD)

Those transforms are employed uniquely, so as to scatter the watermark bits throughout the frame that is transformed for achieving high degrees of transparency and robustness. There are two reasons for this scheme uniqueness:

- The distributed formation of the wavelet coefficient matrix
- The selection of the off-diagonal positions of the singular value matrix to embedbits of the watermark

Various musical clips are used to demonstrate transparency, robustness and high data payload of the suggested algorithm.

Jayanthi *et al.* (2009) present a moment-based normalization public image watermarking algorithm. The proposed moment-based normalization is invariant to affine geometric distortion in camera, satellite and

biomedical images that are stored as "monochrome bitmap". The watermarking approach depends on the normalization of the image. In this approach, both embedding and extraction of the watermark are performed regarding a normalized image to satisfy the criteria of the predefined moment. The result of the watermarking technique fits applications of public watermarking where the host image cannot be obtained for the extraction of the watermark. This study employed "direct sequence code division multiple access approach" for embedding multiple text information in the transform domains of "DCT" and "DWT". The suggested technique of watermarking reveals the robustness against various attacks forms like shearing, flipping, Gaussian noise, JPEG compression, scaling, affine transform, rotation and processing of signal (Jayanthi *et al*., 2011).

Singh *et al.* (2017) present a scheme of non-blind watermarking by combining methods of DWT and SVD. The 2nd level of DWT on the original image is performed to find LL2 subband. The LL2 subband is divided into 8*8 block size and then each block is converted into its RGB color component. SVD is used on each RGB element of each block and find S component for watermarking. They explained the impact of different noise with different variance and gave a comparative study between them. The experimental results proved that the proposed system has excellent resistance to impact of Gaussian noise, salt and pepper noise.

Ghazvini *et al.* (2017) propose a combined watermarking method based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). In the embedding process, a cover image is decomposed by performing a 2-level DWT and the HL2 subband coefficients are divided into 4×4 blocks, then the DCT is applied to each of these blocks. The bits of the watermark are embedded by predefined pattern_0 or _1 on the middle band coefficients of DCT. After adding watermark, the watermarked image is obtained from the inverse of DCT that is applied to each 4×4 blocks of HL2 subband coefficients. For extraction process, the watermarked image is decomposed with 2-level DWT and DCT, then a correlation between middle band coefficients of block DCT and the predefined pattern (pattern_0 and _1) is calculated to decide whether a 0 bit or a 1 bit is embedded. A genetic algorithm is used to optimize the performance of embedding and extracting parameters. The results of this technique show that it is robust against JPEG attacks.

MATERIALS AND METHODS

Proposed system: The system introduced in this study is based on 2DDWT to conceal (embed) binary watermark image in a cover image of size (512×512). In Fig. 2a shows the host image (Goldhill) while Fig. 2b and c show the two embedded binary images. The embedding process is depicted in Fig. 2d in which the embedded images are concealed inside each of "the wavelet bands (LL, HL, LH and HH)" from the cover image. Figure 3 shows the same details but for the cover image called Lena (Fig. 3).

The proposed embedding system which is shown in Fig. 4 is initiated by introducing the host image of size (512×512) single band to a multi level two-dimensional wavelet decomposition based on Daubechies wavelet transform. The watermark binary images W_{mn}^{1} and W_{mn}^{2} have been resized to a suitable size matched with the size of sub-bands derived from certain decomposition level (first, second or third), then scaled using scaling factor •. For example, if the embedding is implemented using the first level of decomposition m = n = 256, for the second level m = n = 128 while for the third level m = n = 64. Then the embedding process is achieved by arithmetic addition between the resized and scaled watermark images with each sub-band coefficients from the selected level of

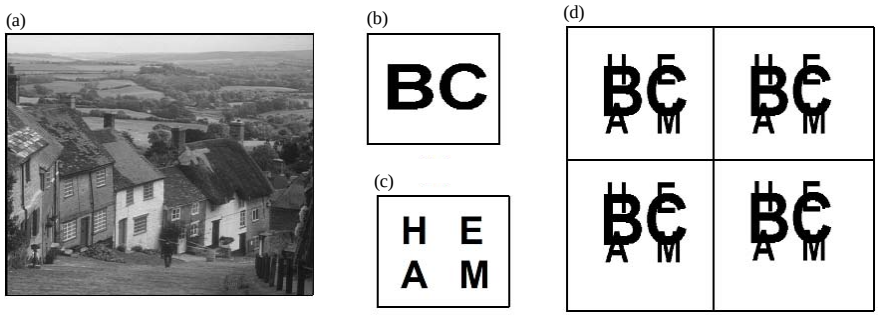

Fig. 2: a) Cover image Goldhill; b) First watermark binary image; c) Second watermark binary image and d) The watermarks extracted from the LL, HL, LH and HH bands

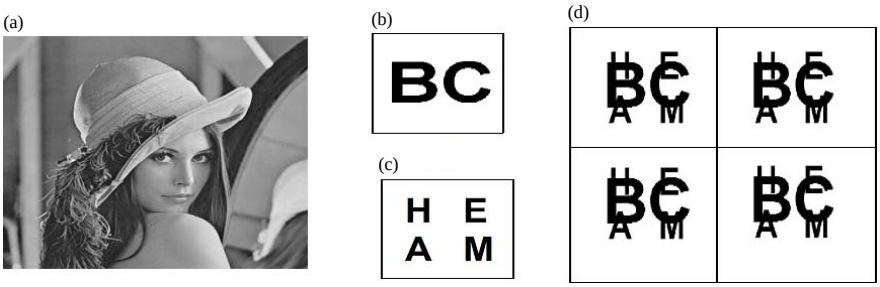

Fig. 3: a) Cover image Lena; b) First watermark binary image; c) Second watermark binary image and d) The watermarks extracted from the LL, HL, LH and HH bands

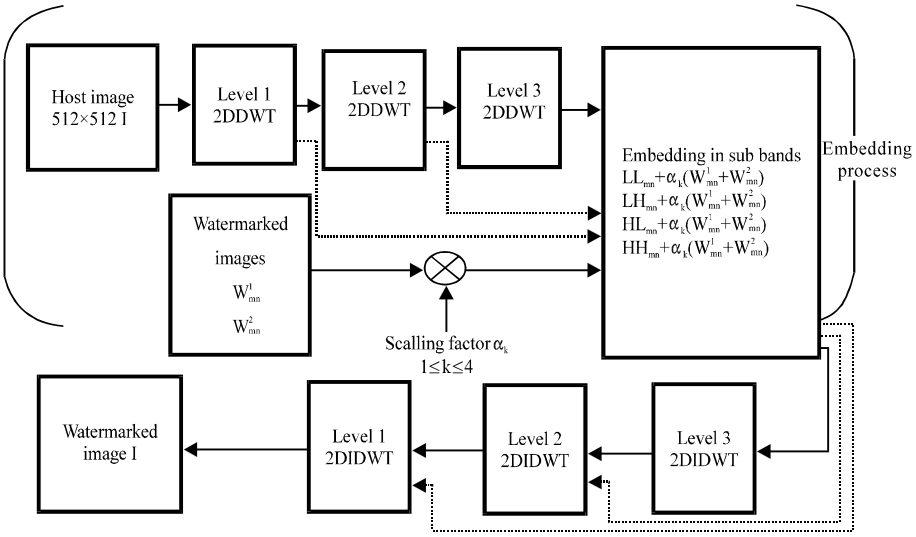

Fig. 4: The block diagram of the proposed embedding process

decomposition. The performance of the proposed system is assessed in terms of (PSNR, Peak to Signal Ratio; SR, Similarity Ratio) for the first, second and third levels sub-bands. Hereby, transparency between the watermarked images and cover image has been evaluated in the embedding process through the use of PSNR. The PSNR value for accepted transparency is (PSNR>20 dB) which is also the minimum required by human the visual system.

The scaling factor vector •(k)is illustrated by the following array: •(k) = {8, 0.5, 0.5, 0.5} where, 1•k•4 where, k is the decomposition sub-band index (1 for LL, 2 for LH, 3 for HL and 4 for HH). The watermarked image in the spatial domain is then generated by calculating the 2D-IDWT for the output image from the embedding process block. The number of composition levels in (2DIDWT) used to construct the watermarked image is the same as that of decomposition levels (2DDWT) employed in the embedding process. The embedding process at 2nd and 3rd levels are derived all from the LL sub-band of its previous level.

Figure 5 shows the stages of watermark images extraction process. Both host and watermarked images undergo multi-level 2DDWT before introducing their outputs to the extraction process block in which corresponding subband coefficients derived from the host image and watermarked image are subtracted to generate the output extracted watermark images. The performance of the proposed system at the extraction stage is measured in terms of (SR, Similarity Ratio) for the first, second and third levels sub-bands. Hereby the SR has been used to evaluate the robustness of the extracted watermark. The value of SR measure of robustness is between 0 and 1, hereby the closest value of SR to one and leads to best robustness. The block diagram of the proposed extraction process is illustrated in Fig. 5.

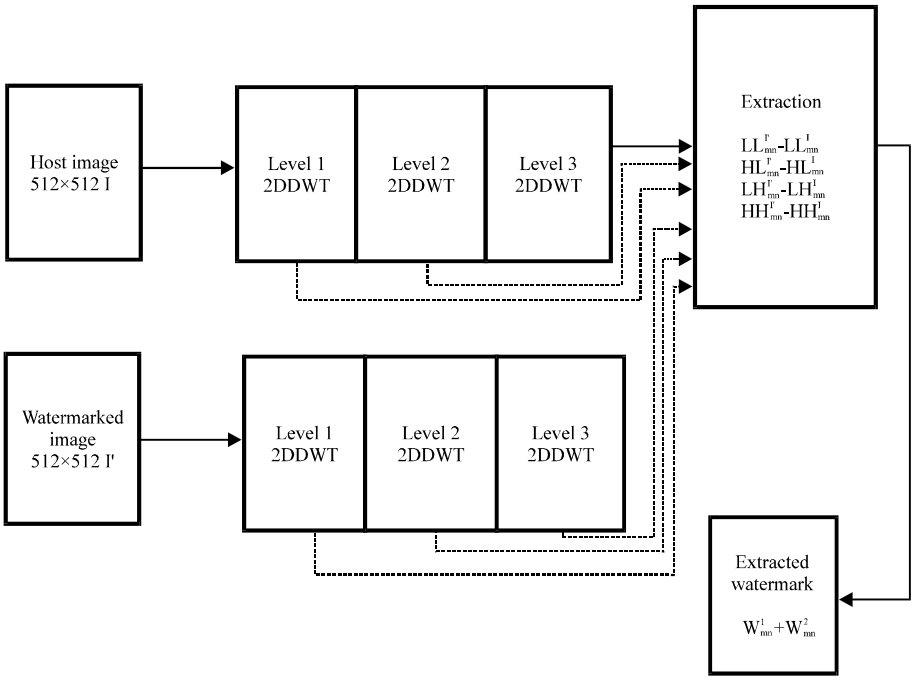

Fig. 5: The proposed extraction system

RESULTS AND DISCUSSION

Performance evaluation: The proposed system has been implemented in MATLAB. The watermarking scheme performance was measured using Eq. 2 performance parameters: perceptual transparency and robustness. Perceptual transparency is measured in terms of PSNR:

$$PSNR(db) = 10\log_{10}\frac{(Max_I)^2}{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[f(i,j)-f'(i,j)\right]} \quad (1)$$

Where:
f(i, j) = The pixel of host image
f'(i, j) = The pixel values of the watermarked image
Max_I = The Maximum pixel gray-level value in the image

The subjective evaluation of extracted watermark is based on, Similarity Ratio (SR):

$$SR = \frac{S}{S+D} \quad (2)$$

Where:
S = The No. of matching pixel values
D = The No. of different pixel values in compared images

For all decomposition levels, five attacks groups are used to test the suggested scheme of watermarking, namely: filter attacks, noise attacks, geometric attacks, JPEG compression and restoration and enhancement attacks. Figure 6a and b contain filter attacks PSNR's values of Lena and Goldhill, respectively. The second level decomposition outperforms the first and third level decomposition in (filter, maximum order filter, median, gaussian filter, average filter). The second level decomposition in minimum order filter shows a better result than the other levels of decomposition. For noise attacks, Fig. 6c and d clarify that the second level of decomposition outperforms both 3rd and 1st levels in the resulted PSNR for both images. The maximum PSNR gain is approximately 0.19 for the Gaussian noise attack. Moreover, Figure 6e and f show the result of geometric attacks. The 2nd level decomposition outperforms the 1st and 3rd level decomposition in both of resize and crop image while the 3rd level is outperforming the other two levels of decomposition in rotate attack. Therefore, they show the PSNR results in superiority of 2nd and 3rd level decomposition in (sharpening and gamma correction) over the 1st level decomposition psnr results. All results of PSNR test values are normalized, so as the values all lies between 0 and 1.The PSNR results of JPEG compression attacks are shown in Fig. 6g and h. The PSNR results of 2nd level decomposition for both images are better than the PSNR results from the other two levels. The maximum PSNR gain is 3.2 from hoster 100 JPEG of Lena image.

For the second performance parameter SR, in Fig. 7a and b show that 3rd level decomposition outperforms levels excepting maximum order filter of filter attack SR

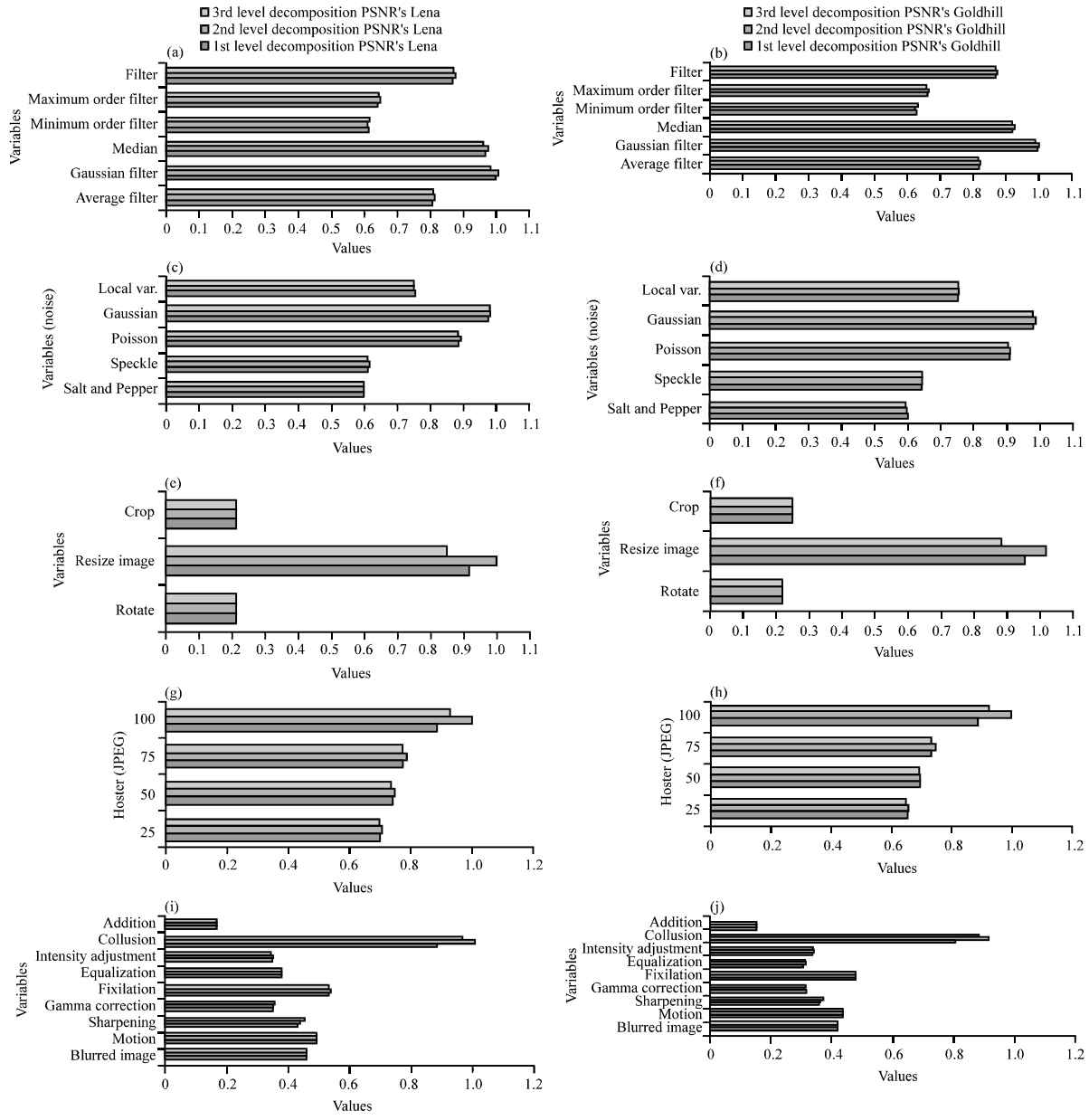

Fig. 6: PSNR's of Lena cover image: a) Filter attack; c) Noise attack; e) Geometric attack; g) JPEG compression attack; i) Restoration and enhancement attack: PSNR's of Goldhill cover image: b) Filter attack; d) Noise attack; f) Geometric attack; h) JPEG compression attack and j) Restoration and enhancement attack

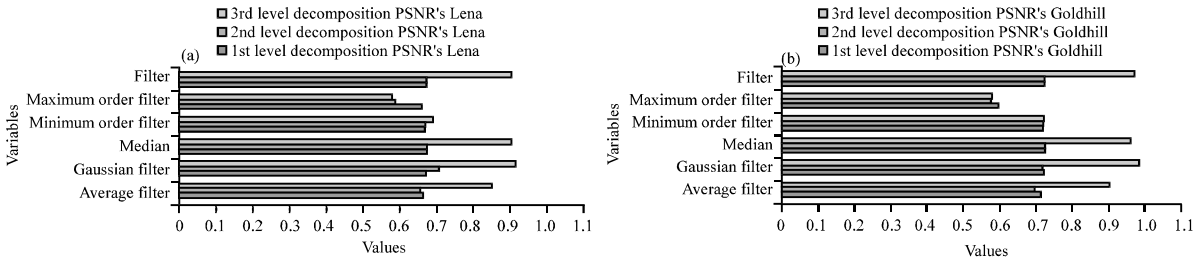

Fig. 7: Continue

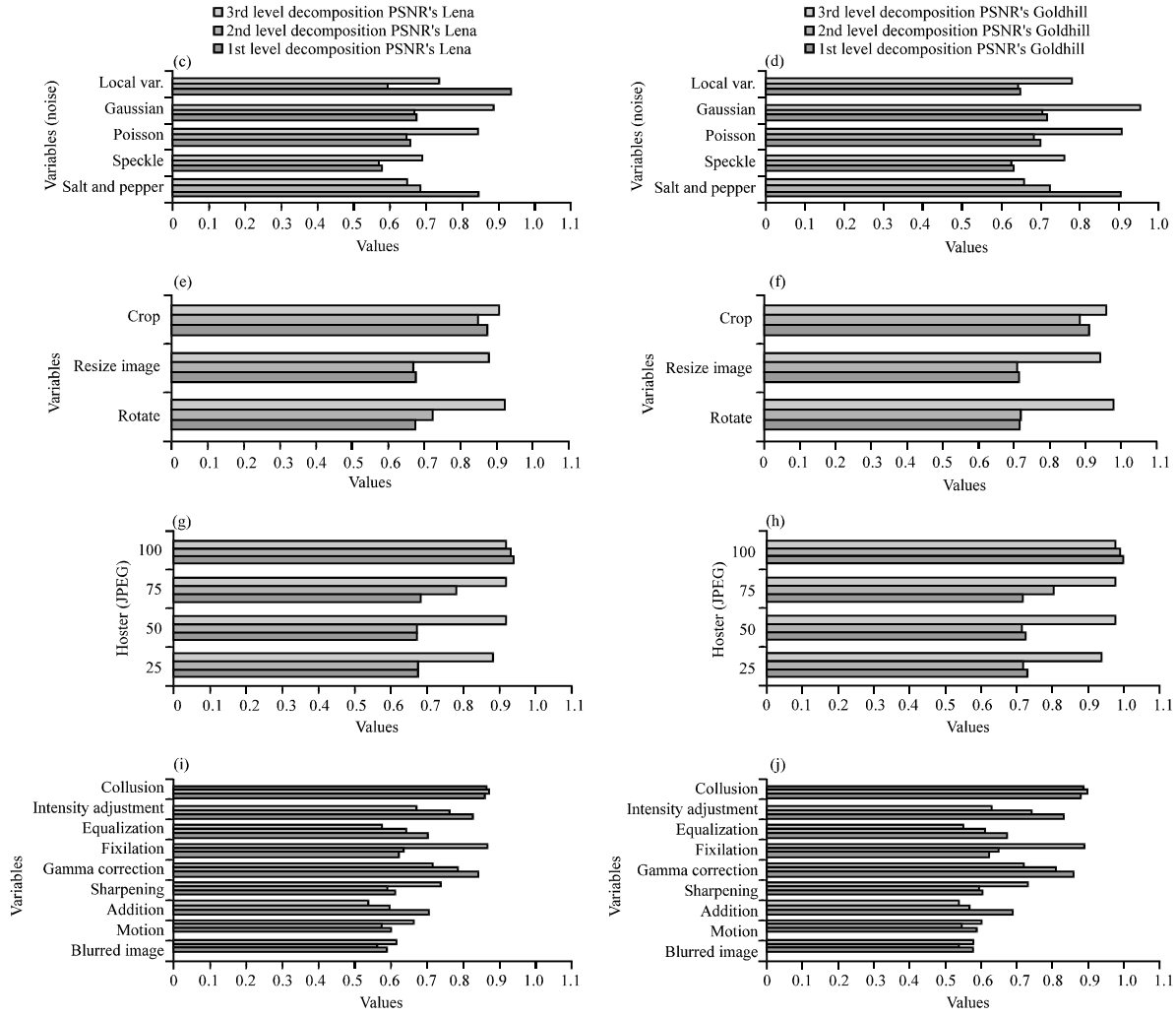

Fig. 7: SR's of Lena cover image: a) Filter attack; c) Noise attack; e) Geometric attack; g) JPEG compression attack; i) Restoration and enhancement attack: SR's of Goldhill cover image: b) Filter attack; d) Noise attack; f) Geometric attack; h) JPEG compression attack and j) Restoration and enhancement attack

results. The maximum similarity gain attained is 0.596. The 3rd level decomposition shows better SR results using noise attacks over the other two levels of decompositions, as illustrated in Fig. 7c and d. The SR results of geometric attacks show that the 3rd level decomposition is better than the other two levels as illustrated in Fig. 7e and f. The SR results derived from JPEG compression attacks are shown in 6g and h. In this Fig. 7, the 3rd level-based watermarking system outperforms the other two levels of decomposition with maximum SR gain of 0.258. Finally, the results of SR derived from restoration and enhancement attacks show the superiority of 3rd level scheme over the 1st level and 2nd with maximum similarity ratio gain of 0.289.

CONCLUSION

A watermarking scheme was proposed based on multilevel wavelet decomposition. The three levels of decompositions were used to embed two binary watermark images. The watermarked images were exposed to five hostile attacks groups. The third level decomposition watermarking system outperforms the other levels in terms of robustness while it shows comparable results in terms of transparency with other levels. As a result, the 3rd level is recommended for watermarking schemes.

As a future work, to determine an optimum solution for the research objective, the researchers will consider optimization soft computing algorithms

proposed in the researches (Al-Dawoodi, 2015; Al-dawoodi and Mahmuddin, 2017; Mahmuddin and Al-Dawoodi, 2017).

REFERENCES

Abdullatif, M., A.M. Zeki, J. Chebil and T.S. Gunawan, 2013. Properties of digital image watermarking. Proceedings of the 2013 IEEE 9th International Colloquium on Signal Processing and its Applications, March 8-10, 2013, IEEE, Kuala Lumpur, Malaysia, ISBN:978-1-4673-5608-4, pp: 207-210.

Al-Dawoodi, A.G.M., 2015. An improved Bees algorithm local search mechanism for numerical dataset. Master Thesis, University Utara Malaysia, Changlun, Malaysia.

Al-Haj, A., 2007. Combined DWT-DCT digital image watermarking. J. Comput. Sci., 3: 740-746.

Al-Haj, A., 2014. An imperceptible and robust audio watermarking algorithm. EURASIP. J. Audio Speech Music Process., 2014: 1-12.

Al-dawoodi, A.G.M. and M. Mahmuddin, 2017. An empirical study of double-bridge search move on subset feature selection search of bees algorithm. J. Telecommun. Electron. Comput. Eng., 9: 11-15.

Deb, K., S. Al-Seraj, M. Hoque and I.H. Sarkar, 2012. Combined DWT-DCT based digital image watermarking technique for copyright protection. Proceedings of the 2012 7th International Conference on Electrical and Computer Engineering, December 20-22, 2012, IEEE, Dhaka, Bangladesh, ISBN: 978-1-4673-1434-3, pp: 458-461.

Ghazvini, M., E.M. Hachrood and M. Mirzadi, 2017. An improved image watermarking method in frequency domain. J. Appl. Secur. Res., 12: 260-275.

Gupta, P., 2012. Cryptography based digital image watermarking algorithm to increase security of watermark data. Int. J. Sci. Eng. Res., 3: 1-4.

Jayanthi, V.E., V. Rajamani and P. Karthikayen, 2011. Performance analysis for geometrical attack on digital image watermarking. Intl. J. Electron., 98: 1565-1580.

Jayanthi, V.E., V.M. Selvalakshmi and V. Rajamani, 2009. Digital watermarking robust to geometric distortions in biomedical images. Proceedings of the 2009 International Conference on Control, Automation, Communication and Energy Conservation, June 4-6, 2009, IEEE, Perundurai, India, ISBN: 978-1-4244-4789-3, pp: 1-6.

Kashyap, N. and G.R. Sinha, 2012. Image watermarking using 3-level Discrete Wavelet Transform (DWT). Intl. J. Mod. Educ. Comput. Sci., 3: 50-56.

Lai, C.C. and C.C. Tsai, 2010. Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans. Instrument. Measur., 59: 3060-3063.

Mahmuddin, M. and A.G.M. Al-Dawoodi, 2017. Experimental study of variation local search mechanism for bee algorithm feature selection. J. Telecommun. Electron. Comput. Eng., 9: 103-107.

Makbol, N.M. and B.E. Khoo, 2014. A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. Digital Signal Process., 33: 134-147.

Maraha, H.E.J., 2014. Audio watermarking using dwt of second level decomposition of low frequency and using rms on approximation coefficients. Ph.D Thesis, Cankaya University, Turkey.

Podilchuk, C.I. and E.J. Delp, 2001. Digital watermarking: Algorithms and applications. IEEE. Signal Process. Mag., 18: 33-46.

Ram, B., 2013. Digital image watermarking technique using discrete wavelet transform and discrete cosine transform. Intl. J. Advancements Res. Technol., 2: 19-27.

Singh, R.K., D.K. Shaw and J. Sahoo, 2017. A secure and robust block based DWT-SVD image watermarking approach. J. Inf. Optim. Sci., 38: 911-925.

Song, C., S. Sudirman, M. Merabti and D. Llewellyn-Jones, 2010. Analysis of digital image watermark attacks. Proceedings of the 2010 7th IEEE International Conference on Consumer Communications and Networking, January 9-12, 2010, IEEE, Las Vegas, Nevada, USA., ISBN: 978-1-4244-5175-3, pp: 1-5.

Tao, P. and A.M. Eskicioglu, 2004. A robust multiple watermarking scheme in the discrete wavelet transform domain. Proc. SPIE., 5601: 133-144.

Thapa, M., D.S.K. Sood and A.M. Sharma, 2011. Digital image watermarking technique based on different attacks. Intl. J. Adv. Comput. Sci. Appl., 2: 14-19.