International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.107-118
http://dx.doi.org/10.14257/ijsia.2016.10.5.10

Digital Image Watermarking Based On Joint (DCT-DWT) and Arnold Transform

Majdi Farag Mohammed El Bireki[1], M. F. L. Abdullah[2], Ali Abdrhman M. Ukasha[3] and Ali A. Elrowayati[4]

[1,2,4]*Department of Communications Engineering, Faculty Electrical & Electronic Engineering,Universiti Tun Hussein Onn Malaysia, Malaysia*
majdi_elbreki@yahoo.com, faiz@uthm.edu.my, elokshy@yahoo.com
[3]*Faculty of Engineering and Technology, Electronics & Computer Engineering Department, Sebha University, Libya*

Abstract

The researcher has adopted a digital watermarking technique which operates in the frequency domain: a hybrid watermarking scheme based joint discrete wavelet transform – discrete cosine transform – (DWT-DCT). Its main objective is to test whether this technique can withstand attacks (its robustness) and invisibility (its imperceptibility), achieved by taking DCT of the DWT coefficients of the LL mid-frequency sub-bands from its band. To ensure security, the secret code (watermark) is scrambled using the Arnold transformation which is embedded in the original host image; only gray-scale digital images are used. The results of this research reveal that the secret code (watermark) is strong enough against threats (noise). Comparative results are measured using signal-to-noise ratio criterions, mean square error and normalized cross correlation. Simulated experimentation is done in Matlab.

Keywords*: Digital watermarking, DWT-DCT transform, Arnold transformation*

1. Introduction

The increasing numbers of internet users everywhere in the world have imposed many menaces on the protection of the obtainable digital data. Researchers and scholars in the area of cyber security are challenged to create new techniques to block such a menace. Hence, this research performs digital watermarking as a way for safeguarding different kinds of information like texts, images, audios or videos. It is basically done by concealing particular amounts of visual images by placing invisible marks such as copyright information to restrain any unlawful use of these images.

An experiment has been processed on a watermarked image prior and after noised by attacks such as blurring. Frequently used transforms are the discrete Fourier transform, discrete wavelet transform and discrete cosine transform. [1,2,3]. Without having lost its quality, digitally stored information can be transmitted easily [4].

Watermark embedding methods are commonly applied in spatial domain [5, 6] or in frequency domain [7,8]. Whereas the first is renowned for its weakness in the common image threats such as (JPEG) compression, the last (the frequency domain), has better quality when it comes to image watermarking by altering their coefficients. This transformed domain watermarking technique must have to undergo certain steps: 1) the image must be transformed; 2) how to embed the watermark and 3) watermark recovery scheme.

Robustness requirements of digital watermarking algorithms operated in frequency domain are far better off than spatial domain techniques [3]. In order to have an efficient watermarking technique, it should be concealed; it can be used together with the original

ISSN: 1738-9976 IJSIA

image and should provide correct data [6]. To check whether it's effective, simulation (using Matlab) was used for experimenting various image processing techniques (to insert and extract watermarks).

This research will cover mainly on digital image watermarking. Unnoticeable identifying marks are added to ensure ownership or copyright information [10]. It is then a necessity to evaluate these watermarking techniques whether they cannot be seen by the naked eye, they are easy to recover and can withstand various attacks. The aim is to perform a watermarking scheme and to assess the effects of several image processing techniques as attacks (noise or geometrical).

A combined DWT-DCT transform method was performed to embed the watermark. The secret image is scrambled using Arnold transformation. DCT is applied on both original host image and to the secret image/watermarked image after scrambling. This paper is organized in this manner: Section 2& 3 briefly describes various domain transforms while Section 4 proposes the hybrid DWT-DCT-Arnold Transforms technique. Section 5 deals with the applied measures, Section 6 the experimental results and Section 7 conclusions.

2. Joint Transforms

Watermarking scheme based on transform domain basically adapts transform coefficients from the bits of the watermark image. Generally, DCT and DWT are initially performed and then transform the image into the spatial domain. Grayscale images are mostly preferred in watermarking schemes. One of the advantages in DCT-based algorithms is its high capacity of hiding data. Though these algorithms withstand various attacks (robust), it is also tamper-prone and can easily deteriorate the quality of the watermarked image. DWT-based algorithms have better image quality but are vulnerable to various attacks. To solve these problems, a hybrid digital watermarking scheme basing on DWT-DCT is proposed. This combined (hybrid) technique has been used in signal processing widely. To ensure significant form of security, an image scrambling technique has been added. This scrambling technique is applied to disturb the position of the image's pixel, making it a messy image which subsequently makes the original image unidentifiable [8,11,12,13].

- **Discrete cosine transform (DCT):**

A signal is converted into elementary frequency components representing the sum of sinusoids in diverse magnitudes and frequencies of an image. Signal processing, compression, image processing, *etc*. are various applications that can be provided by this transform [4,5,7,12]. A DCT - applied image forms low-, mid- and high frequency sub-bands.

Important and major visible regions of the image are inside the low-frequency sub-bands while high frequency regions of the image can be eliminated when attacks (compression and noise for instance) are applied. When these middle frequency sub-band coefficients are modified or changed slightly, watermark is then embedded in this sub-band so that the watermark stays robust when compressed and the desired or noticeable quality of the image will not be affected or altered at the same time [9,10,12] .

- **Discrete wavelet transform (DWT) :**

One of the advantages of wavelet transform is that it can be used to find a way of dealing difficult problems of computers, mathematics and physics, decomposing them into basic form and yielding high precision reconstruction performance [13].

Wavelets are special functions representing signals. When level wavelet decomposition is applied to an image, 2-D DWT gets ten sub-bands: LL_3, HL_3, LH_3, HH_3, HL_2, LH_2, HH_2, HL_1, LH_1 and HH_1. These sub-bands are characterized by: 1) low frequency sub-

bands which occupy almost all of the energy of the image's signal and 2) high frequency sub-bands which include texture, edge and outline of the image. Lower frequency sub-bands contain most of the image' energy but when too much watermarks in these sub-bands are embedded, the quality of the image may deteriorate; however, it could boost its robustness. Human eyes are not in all times perceptive to alterations in these sub-bands. Watermark embedding is done here because it can't be detected by the human eye and it has an acceptable achievement level of imperceptibility and robustness.

3. Arnold Transform

Pixels' positions are altered and if done a number of times, the appearance of the image becomes messy when this scrambling technique is used. It requires the height or width (N x N) of the image that needs to undergo the process. The periodic trait of the Arnold Transform (see Table 1) has much to do with the dimension of the image to be decoded depending on the transformation time (T) , which also alters according to the image' dimension. Image iterations occur when this technique is applied. A secret key derived from this iteration number is used to encrypt and extract the secret image [8]. If some hackers detect the watermark signal, they need to use this key to get the watermark. Even if they have the key, they still have to undergo a lot of testing to recover the original watermark data. Thus, security and concealment of the watermark is further improved by the use of this scrambling technique. Thus defined, 2-D Arnold transform for an N X N image is

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} . \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N} \quad (1)$$

x, y∈ {0,1,…, N-1}, (x, y) and (x′, y′) are the coordinates of the pixels before-and-after scrambling.

Table 1. 2- D Arnold Transform Periodicities

N	10	25	50	60	125	128	256	480	512
TN	30	50	150	60	250	96	192	120	384

4. Description of the Algorithm

A scrambled binary watermark logo(CS) using Arnold transform is embedded in a three level DWT selected coefficient sets of a transformed original image (gray level image, 1024*1024). Use a key to embed the scrambled watermark. In the extraction steps, a pre-filtering method is used (Medfilt filter) to the watermarked image (which may have been attacked) in order to establish clear difference between the host image and watermarked image. Extraction process of the DCT mid-frequencies of each sub-band (approximation) follow the same process in embedding the watermark.

This research aims to achieve better robustness and imperceptibility of the watermarked image against digital signal processing and noise addition attacks.

- **The embedding algorithm**

This joint wavelet and cosine transform in embedding watermark information to the original image is used to compare with the method of Amirgholipour,*et al*, 2009 [14]. In their experiment, they used the mid-frequency coefficients (details) in embedding their watermark data and its extraction, divide the sub-bands into 4x4 blocks whereas the proposed method chose the approximation frequency coefficients and divided the sub-bands into 8x 8 blocks. DWT is excellent in choosing

the most appropriate sub-bands in order to achieve imperceptibility and robustness. Apply blocked-DCT on selected bands when embedding the watermark into the chosen mid-frequencies of every block. By doing so, watermarked image' robustness will be increased against various geometrical or noise attacks and suppressing the effects of these attacks. This algorithm is done using the MATLAB.

- **Scrambled watermark**

The embedded watermark is a two dimensional image. The watermark is scrambled first to ensure that it can withstand re-sampling, clipping, *etc*., when embedded and improve the watermark's robustness [8]. Because of its simplicity, periodicity and easy usage [cat mapping], Arnold transform is used as a pre-treatment method to indicate the watermark [8].

- **The embedding process**

Watermarking process starts through the application 3-levels DWT to the original image. Pseudorandom sequences are embedded in the mid-frequencies after applying block based DCT to the chosen DWT coefficient sets. Figure 1 illustrates the watermark embedding procedure.

Use the approximation sub-band LL to embed the watermark data. Figure 2 illustrates how 3-level DWT is applied to the original image to obtain a non-overlapping multi-resolution DWT coefficient sets from one level to another level.

- Perform DWT on the original image, decomposing it into 4 coefficient sets (multi-resolution) LL_1, HL_1, LH_1 ,HH_1.
- Perform DWT to approximation LL_1 coefficient sets to get four smaller coefficient sets LL_2, HL_2, LH_2, HH_2.
- Perform DWT to approximation LL_2 coefficient sets to get four smaller coefficient sets LL_3, HL_3, LH_3 , HH_3; select HL_3 and LH_3 as sub-bands.
- Divide the sub-band HL_3 and LH_3 into 8x8 blocks.
- Apply DCT to each block in the selected coefficient sets HL_3 and LH_3 and use the highest N value of the HPF (zonal sampling).
- The watermark logo CS will be scrambled using the Arnold algorithm for a number of times to obtain the scrambled watermark Ws (i , j), which will serve as the secret key.
- Prepare the scrambled watermark image's size and direction of 0 and 1; then create two independent pseudorandom sequences using a key: one which will be used in embedding watermark bit 0 and the second to embed watermark bit 1.
- Embed the scrambled watermark logo in the mid-band coefficients of the DCT transformed 8x8 blocks of the chosen DWT coefficient sets of the host image.
- Apply/ inverse DCT on all blocks
- Perform/inverse DWT on the DWT transformed image coefficient sets to obtain the original image that has the watermark.

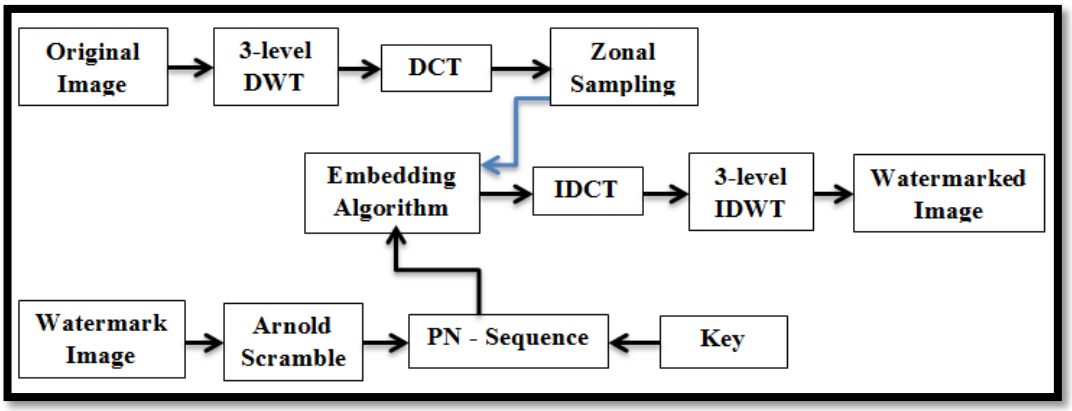

Figure 1. Watermark Embedding Procedure using Hybrid DWT-DCT and Arnold Transform

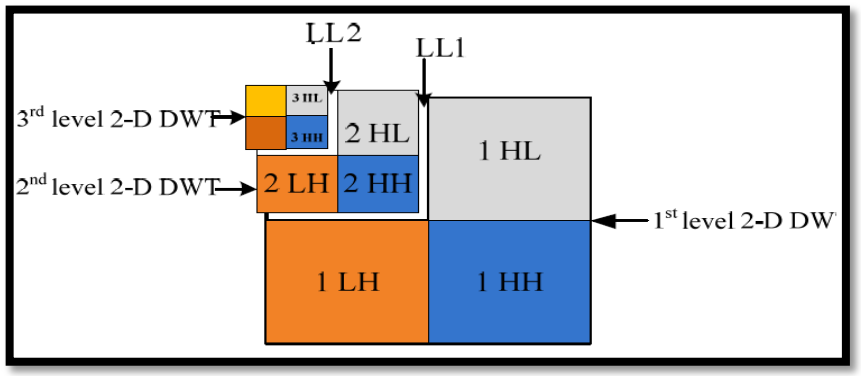

Figure 2. 3 Level DWT Decomposition Application of the Original image

- **Watermark ExtractionAalgorithm**

The original host image is not necessary or needed to extract the watermark because this hybrid DWT-DCT is blind watermarking process. Extraction method is identical with the embedding process. Pre-filter before DWT transform is applied to distinguish watermark data from original image. See Figure 3 for watermark extraction process.

- Perform med-filtering of the matrix A in two dimensions. MEDFILT2 pads the image with zeros on the edges, making the median representation for the points inside the range of [M N]/2 of the edges may appear changed.
- Apply DWT on the pre-filtered watermarked image decomposing it into four multi-resolution coefficient sets LL_1, HL_1, LH_1 and HH_1.
- Apply DWT again to approximation LL_1, coefficient sets to get four smaller coefficient sets LL_2, HL_2, LH_2 and HH_2.
- Perform DWT again to approximation LL_2 coefficient sets to get four smaller coefficient sets LL_3, HL_3, LH_3 and HH_3 ; choose sub-bands HL_3 and LH_3
- Divide the sub-bands HL_3, and LH_3 into 8x8 blocks.
- Apply DCT to every block in the selected coefficient sets HL_3 and LH_3 and use the highest N value of the HPF (zonal sampling).
- Recreate 2 pseudorandom sequences 0 and 1with use of the same key used during the embedding process.
- Use the extracted watermark bits to reconstruct the scrambled watermark
- Use the same number of times scrambling the extracted watermark

(Arnold) in order to obtain the scrambled watermark; compare the original from the extracted watermark on its similarity.

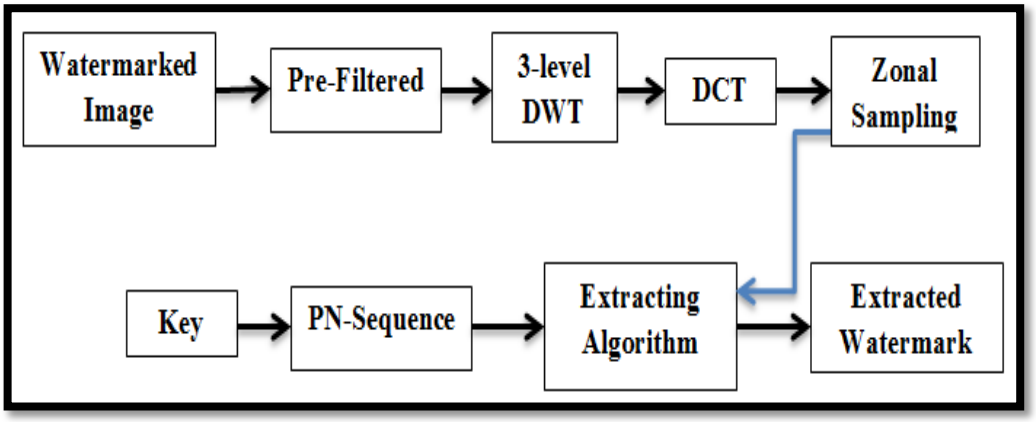

Figure 3. Extraction Procedure of the Watermark using Joint DWT-DCT

5. Applied Measures

A. Mean square error (MSE)

It is the square of the error between the original and watermarked image; distortion in the image can be measured using:

$$MSE\left(I, \tilde{I}\right) = \frac{1}{(n*m)} \sum_{i=0}^{n} \sum_{j=0}^{m} (I(i,j) - (\tilde{I}(i,j))^2 \quad (2)$$

Where $I(i,j)$= original image ; $\tilde{I}(i,j)$ = watermarked image.

B. Imperceptibility

The original image and the watermarked image' quality (statistical difference) is measured using PSNR. The PSNR between the original and reconstructed images is expressed in the equation:

$$PSNR\left(I, \tilde{I}\right) = 10 \log_{10} \frac{(L-1)^2}{MSE\left(I, \tilde{I}\right)} \quad (3)$$

Where L = grey-level number; I = original mage; $\tilde{I}$ = watermarked image

C. Robustness

Watermarking method's robustness is assessed by applying attacks (geometrical, noise, image compression) on the watermarked image and evaluates the similarity of the extracted watermark to the original watermark.

$$NCC = \frac{\sum_i \sum_j [W(i,j).(W'(i.j)]}{\sum_i \sum_j [W(i,j)]^2} \quad (4)$$

Where $W(i,j)$ = original watermark; $W'(i.j)$ = extracted watermark after several transformations.

6. Experimental Results

Our results are shown in this section. We tested the imperceptibility of the host image which has been watermarked and the robustness of the watermark when attempted to be messed up, destroyed, removed or degraded. Three major attacks were executed: Blurring (motion), noise (salt and pepper) and image compression (JPEG). Even only a few, they represent most common attacks.

Experiments conducted used a 1024 x 1024 host image "Tools" (Figure 4) and 256 x 256 of 'CS' as the watermark image (Figure 5) to test the robustness of the method. Figure 6 shows the watermarked Tools and the extracted watermark without any attacks (Figure 7).

Figure 4. Original Host Image Tools

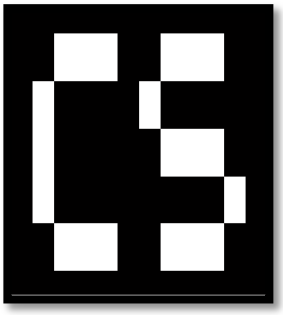

Figure 5. Watermark Image

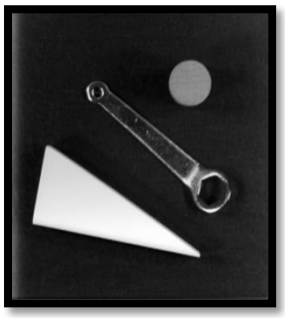

Figure 6. Watermarked Image Tools

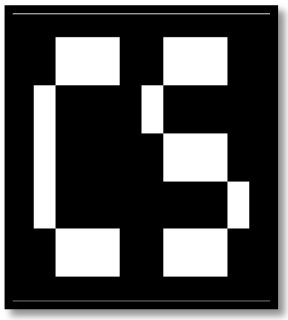

Figure 7. Extracted Watermark Image CS

Figures 8 -12 depict a host of attacks such as motion filter, JPEG and Salt and Pepper. Watermarked image' imperceptibility qualitatively high. A PSNR representation higher than 35dB is within an acceptable level of degradation, which also means that it is almost not seen by the HVS. To remove the salt and pepper attack, a medfilter is used to obtain the extracted watermarked image. The extracted watermarks after undergoing various attacks are shown in Figures 13-15 with Normalized Cross Correlation values as a measure for robustness. A correlation coefficient of 0.75 or above is generally acceptable.

Table 2 shows the summary of the results of the quality of the watermarked image (PSNR), the similarity between the original and extracted watermark (NCC) and the similarity of the images (MSE). The proposed algorithm is compared with that of the work of Amirgholipour, *et al*, 2009 [14].

The motion filter is applied to the watermarked image. The recovered watermark show good similarity with original watermark. Lossy JPEG compression is performed with a compression index ranging from 0 to 100, where 0 is the best compression and 100 is the

best quality. Even subjected to salt and Pepper attack, still we find a good resemblance with the original watermark. In all of the above attacks, we recovered good visual watermarks.

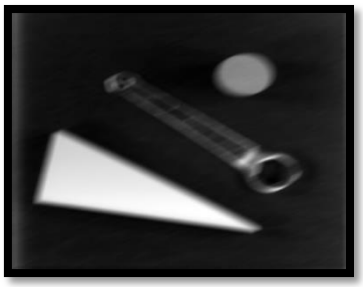

Figure 8. Blurring Attack

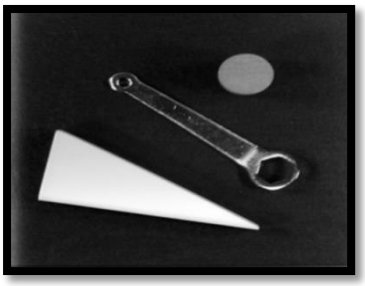

Figure 9. Restored Watermarked Image

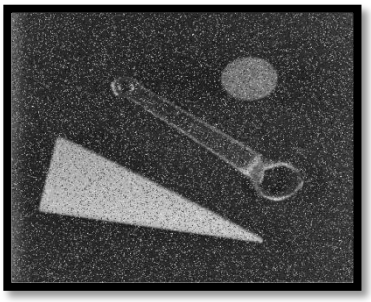

Figure 10. Salt and Pepper Attack

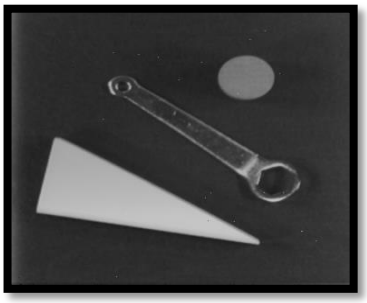

Figure 11. Watermarked Image after using Medfilt

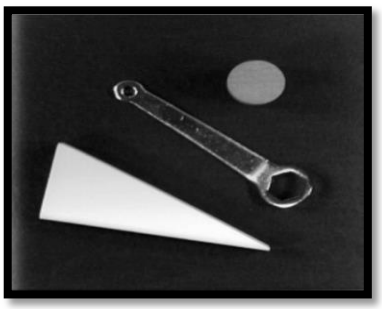

Figure 12. JPEG Attack

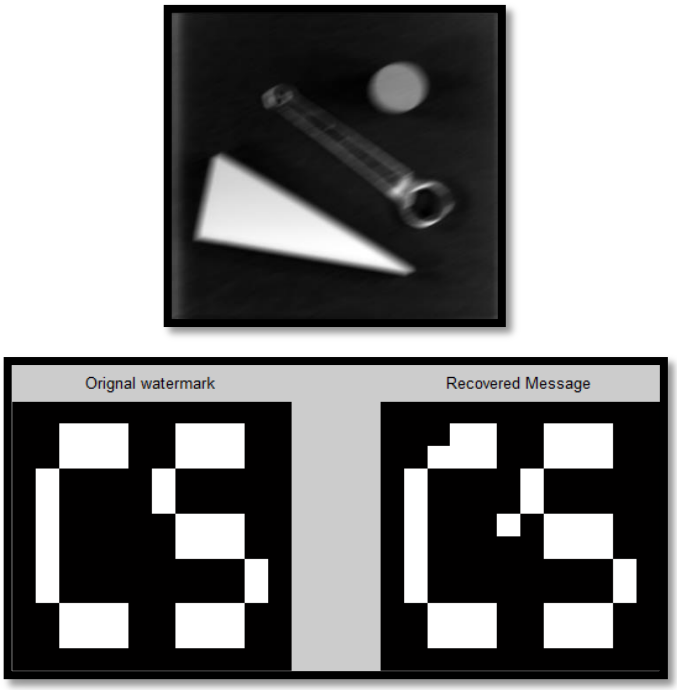

Figure 13. Extracted Watermark with the Proposed Algorithm

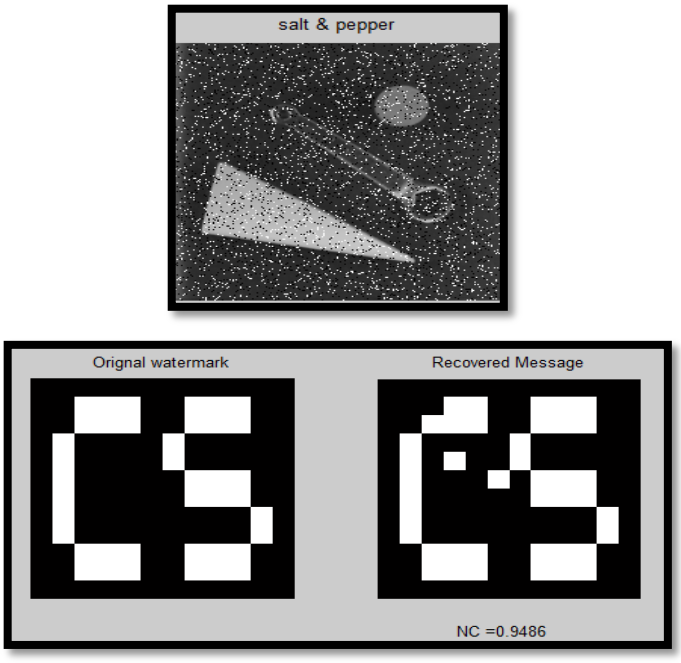

Figure 14. Extracted Watermark with the Proposed Algorithm

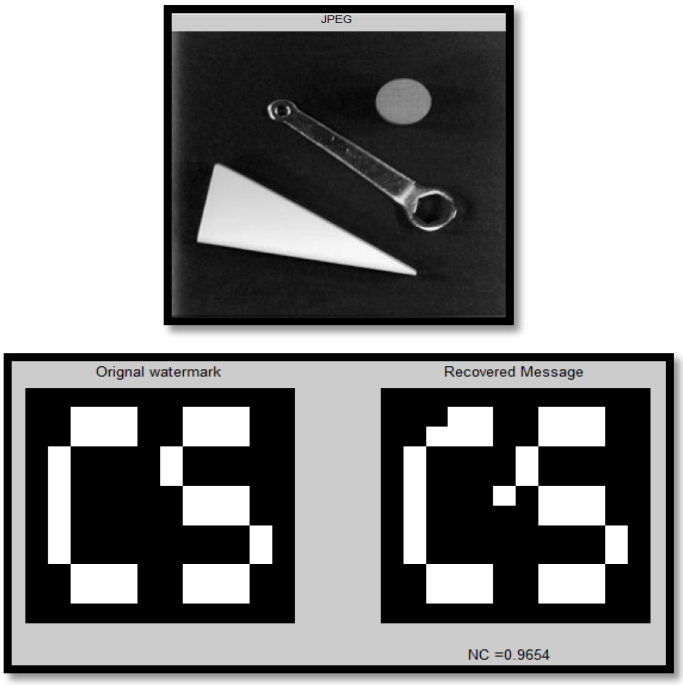

Figure 15. Extracted Watermark with the Proposed Algorithm

Table 2. Results of the Applied Measures Achieved using DWT-DCT-Arnold Transform

Type of attack	Comparative Results	PSNR	MSE	NCC
Blurring	**Proposed algorithm**	51.9559	0.4145	0.9730
	Amirgholipour	51.0890	0.5060	0.9665
Salt and Pepper	**Proposed algorithm**	42.1678	3.9473	0.9486
	Amirgholipour	41.8662	4.2311	0.7921
JPEG	**Proposed algorithm**	48.8498	0.8474	0.9654
	Amirgholipour	43.5999	2.8385	0.8423

7. Conclusion

In this paper, a watermarking algorithm based on hybrid technique is proposed. Our objective is to perform watermarking by taking DCT of the DWT coefficients of the LL mid frequency sub- bands of DWT and test whether quality of the original image has not been distorted by the presence of the watermark. Second is to test whether the watermark withstands various digital signal processing attacks. We embedded the watermark in 3 level DWT sub-bands on the original image (2-D) then applied DCT on the selected DWT sub-bands. Watermark image is scrambled first using Arnold transform.

These combined techniques and our proposed algorithms displayed good results when tested on its imperceptibility and robustness except when subjected to noise attack (salt and pepper). Comparative results show that the proposed algorithm is robust and imperceptible, showing better results. For future research work, embedding multiple watermarks in 3 level DWT mid-frequency coefficients will investigated so that the watermark image can resist an increased amount of attacks not only to blurring, noising and compression.

References

[1] R.Ibrahim and T. S.Kuan, "Steganography Imaging (SIS): Hiding Secret Message inside an Image". Proceedings of the World Congress on Engineering and Computer Science, San Francisco, USA. **(2010)**.
[2] L. Baisa and R.R. Manthalkar Gunjal, "An Overview of Transform Domain Robust Digital Image Watermarking Algorithms", Journal of Emerging Trends in Computing and Information Sciences, **(2010)**.
[3] C.C Lai and C.C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE Trans. on Instrumentation and Measurement, vol. 59, no. 11, **(2010)**, pp. 3060-3063.
[4] P. Satyanaraya Murty and R. Kumar, "A Robust Watermarking Scheme Using Hybrid DWT-DCT-SVD Technique", IJSNS, vol. 10, no. 10, **(2010)**, pp. 187-192.
[5] Z. Tang. and X. Zhang, "Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies", Journal of Multimedia, vol. 6, no. 2, **(2011)**.
[6] G.S. Kalra, R. Talwar and H. Sadawarti, "Blind Digital Image Watermarking Robust Against Histogram Equalization", Journal of Computer Science, vol. 8, no.8, **(2012)**, pp. 1272- 1280.
[7] M.F.L. Abdullah, A. A. M. Ukasha and M.F. Mohammed Elbireki, "Image Compression Technique using DCT, FFT Transform", Presentation in National Conference on Electrical and Electronic Engineering (NCEEE) **(2012)**.
[8] G Yuxi and W Yanmin, " DWT Image Watermarking Algorithm Based on Scrambling Algorithm", IEEE Proceedings, World Automation Congress, **(2012)**, pp.1-4.
[9] D.V.N Koteswara Rao, Y..Madhuri, S.V. Rajendra Kumar, and Y.V. Suresh Babu, "Robust Image Watermarking using DCT & Wavelet Packet Denoising" , Dept. of Electronics and Communication Engineering, SACET,Chirala, International Journal of Scientific and Engineering Research Vol. 3, Issue 5, May-2012.
[10] K. Deb, M.S. Al-Seraj, M.M. Hoque and M.I.H. Sarkar, "Combined DWT-DCT Based Digital Watermarking Techniques for Copyright Protection", IEEE Publication, 7th International Conference on Electrical and Computer Engineering **(2012)**.
[11] A. Akter,.T Nur-E and M.A. Ullah, "Digital Image Watermarking Based on DWT-DCT; Evaluatefor a New Embedding Algorithm", IEEE Publication, International Conference on Informatics, Electronics and Vision (ICIEV), **(2014)**, pp. 1-6.
[12] M Farag, M Elbireki, M. F. L. Abdullah and A.A.M Ukasha, "Adopting A Robust Watermarked Image Against Cyber Security Threats Using DCT and Ramer Method", Fifth International Conference on Intelligent Systems, Modelling and Simulation (ISMS) **(2014)**, IEEE.
[13] A Ukasha, Majdi Elbireki, and M. Abdullah, "Contour Extraction & Compression from Watermarked Image using Discrete Wavelet Transform & Ramer Method", International Conference on Image Processing and Electronics Engineering (ICIPEE'2013), Penang (Malaysia), **(2013).**
[14] S K. Amirgholipour and A. R. Naghsh-Nilchi, "Robust Digital Image Watermarking Based on Joint DWT-DCT", International Journal of Digital Content Technology and its Applications, vol. 3, no.2, **(2009)**.

