Journal of Engineering and Applied Sciences 11 (Special Issue 2): 3227-3232, 2016
ISSN: 1816-949X
© Medwell Journals, 2016

Digital Image Watermark Authentication Using DWT-DCT

[1, 2]Atheer Bassel and [1]Md. Jan Nordin
[1]Center for Artificial Intelligence Technology, Faculty of Information Science and Technology, Universitiy Kebangsaan Malaysia, 43600 Bangi, Selangor Darul Ehsan, Malaysia
[2]University of Anbar, AlAnbar, Iraq

Abstract: Multimedia communication is widely used nowadays; it has been used in most of life fields. Great importance has been given to a new art concerns about hiding a secret message inside pictures. The watermarking is as a method of concealing digital information security in the middle of the multimedia data that is the host image. Discrete Wavelet Transform (DWT) when joined together with discrete Cosine Transform (DCT) delivers the powerful digital watermarking image. There are different types of intrusions that either plunder the actual ownership or demolish the appearance. In this study, the DWT-DCT approach has been proposed so as to establish the secure appearance by concealing the watermark inside the actual image and validate the proprietor's image. Using DWT-DCT and low-bit percentage, the watermark image is inserted and abstracted. Results have been displayed based on the hybrid DWT-DCT for excellent capable digital watermarking image. The expected conclusion of this research is a technique that has the ability to hide the secret data (message) inside the image by using DWT to avoid all the different types of attacks and finally extract the secret data from the image. Two techniques has been used to achieve imperceptibility and robustness of the watermark against certain geometric and non-geometric attacks.

key words: Digital image, watermarking, authentication, multimedia, DWT and DCT

INTRODUCTION

In this work we study the digital watermarking technique, the current proliferation of technology, accessible internet and different image transformation equipment's are susceptible to a large extent, the feasibility of downloading an image from the internet and administering it with the acknowledgement of the actual owner. Hence, validating the image is not only considered as dynamic but also an important research area (Mishra *et al*., 2014). In a watermarking approach, there are two kinds of algorithms: embedding algorithm and extracting algorithm. The embedding algorithm is a mechanism of fastening the digital data with the watermark which can either be a text or an image. In this mechanism, both the host image and the watermark are considered together and the watermark image is embedded inside the host image, therefore safeguarding the host image. Hence, the inserted image can demolish the features of the actual data. Nevertheless, the abstraction algorithm is a mechanism of abstracting the watermark from the watermarked image which is dissimilar to the host image. Hence, the performance of the watermark image is evaluated on the basis of different characteristic specifications, for instance, Normalized Correlation (NC), Peak-Signal-to-Noise-Ratio (PSNR), mean square error (Mishra *et al*., 2014; Lim, 2015).

An advantageous watermarking pattern should captivate the powerfulness and imperceptibility. The first one signifies that the non-cognitive distinctness between the watermarked and the actual report is not noticeable to the human eye. Also, the watermark should not intervene the media that is being safeguarded. Agility highlights that the un-authentic individual should not demolish the watermark nor should make the report not valuable. The watermarks also should be powerful and strong enough to signal execution and intended intrusions. Powerful watermarking has been constructed in a way that is invulnerable against intrusions for instance, noise, cropping, filtering etc. that aim to erase or demolish the watermark apart from deteriorating the viewable feature of the watermarked image considerably. In this manner, it is utilized to safeguard and ascertain the authorship. On contrary, breakable watermarking is introduced to guarantee the adherence and image authorization instead of validating the real ownership. It discovers un-authentic amendment which will either destroy or change the watermark. Semi delicate watermarking integrates the

Corresponding Author: Atheer Bassel, Center for Artificial Intelligence Technology, Faculty of Information Science and Technology, Universitiy Kebangsaan Malaysia, 43600 Bangi, Selangor Darul Ehsan, Malaysia

characteristics of both delicate and powerful watermarking so as to discover un-authentic handling while still being powerful and resistant against authentic handling. The most vital operation for watermarking is the preserving of electronic information ownership authorization. Electronic watermarking supports in the verification of the ownership authorization of the presented image. For frequency realm watermarking, values of precise densities are altered from their actual two distinct arrangement (Cox *et al*., 1997).

Typically in electronic image watermarking, an individual value of the scaling determinant is utilized to introduce the watermark in the complete host image. The local allocation of the actual image is not acknowledged during the introduction process. Nevertheless, this kind of introduction can direct to some unwanted naked relics inside watermarked image (Cox *et al*., 1997; Li *et al*., 2007; Waleed *et al*., 2014). These distortions are recorded mainly in sleek domains because these domains are susceptible to sounds. To lessen these distortions, the scaling determinant should be reduced in the plain domains, therefore influencing the powerfulness of the introduced process. In other domains, enhancing the scaling determinant above a definite margin can cause naked disruptions inside the marked image. Choosing scaling determinant has become an important concern of agreement between imperceptibility and powerfulness (Cox *et al*., 1997) has induced that an individual scaling determinant may not be suitable for disturbing all the coefficients of cover image as various illusory factors may display additional or smaller strength to alteration. Digital watermarking mechanism come under spatial and frequency category depending upon the class in which they are used for introducing the watermark. Spatial category watermark alters the pixels of one or two unplanned chosen subsets of images (Waleed *et al*., 2014).This kind of mechanism proves powerless across average image processing and intrusions such as sound, filtering, compression which might be demolished with less effort by disruption (Waleed *et al*., 2014). The deformities caused by damaged image compression, signal processing function and other intrusions are the average difficulties faced during the utilization and allocation of watermarked image. Therefore, a powerful watermarked image is needed to form support across image deformities of enduring intrusions (Zhang *et al*., 2011). Frequency category is also recognized as transform category for instance, Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Singular Valued Decomposition (SVD) are some of the ordinary categories being introduced (Waleed *et al*., 2014; Shensa, 1992). These categories can be joined together to enhance the efficiency of the frequency category and the powerfulness under the intrusions. Still ordinary research on image watermarking has restricted its analysis to the utilization of accepted mathematical creations for example DCT, DWT and some other composite variants for example DWT-DWT and DWT-DCT. In this study, we highlight the efficiency of hybrid watermarking mechanism for the two joint methods: DWT-DCT and DWT-DWT.

Literature review

Discrete Wavelet Transform (DWT) and Discrete Cosine Transform DCT: Discrete Wavelet Transform (DWT) is a mechanism that is utilized in uncontrolled watermarking mechanism and collateral to transform region watermarking. Wavelet based watermarking is a well-known domain due to its potential against vulnerable intrusions (Gupta and Shrivastva, 2010). DWT partitions the signal in two dimensions: high frequency and low frequency (Dharwadkar and Amberker, 2010; Lim, 2015). A signal is made to pass in between the high pass filter and then access low pass filter to examine the low frequency filter. Outcome from the high and low pass filters deliver DWT coefficients that are employed on the modified real image, acknowledged as Inverse Discrete Wavelet Transform (IDWT) (Karniawan and Purnama). Typically, the introduction of watermark inside the image is gained by contemplating the DWT coefficients of the disintegrated image with the coefficients that have the sufficient area suitable enough for the introduction of the watermark. Kumar *et al*. (2012) Suggested against the intrusion categories so as to ignore image deformities created by intrusions and the utilization of sub band coefficients may alter it by channel sound. According to Gupta and Shrivastva (2010), correlation coefficient values do not get enhanced amid the actual watermarking and the extorted watermarked.

DCT is a well-known mutation function that alters a signal from the spatial to the frequency realm and so far it has been utilized in the JPEG class for the abstraction of image due to its efficiency. It alters actual data into the actual spectrum ignoring the difficulties of repetition. The well-known block dependent DCT alters the segments into un-stretched blocks and employs the DCT to every individual block.

DCT and DWT (Shefali *et al*., 2008; Lal *et al*., 2015) alterations, so far have been widely used in profuse digital signal processing functions. Discrete cosine transform is a mechanism for altering a signal into basic frequency categories (Dharwadkar and Amberker, 2010; Migdadi *et al*., 2015). An image is highlighted as an average of sinusoids of different densities and weights. ‘x’ which is being utilized as an input image, DCT coefficients for the altered output image ‘y’ are calculated according to Eq. 1 as represented below. In the given equation, ‘x’ is an input image of N x M pixels and x (m, n) is the strength of the pixel in row m and column n of the image while y (u, v) signifies the DCT coefficient in row u and column v of the DCT matrix.

$$y(u,v)=\sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_u\alpha_v\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} x(m,n)\cos\frac{(2m+1)u\Pi}{2M}\cos\frac{(2n+1)v\Pi}{2N} \quad (1)$$

Where:

$$\alpha_u=\begin{cases}\frac{1}{\sqrt{2}} & u=0, u=1,2,\ldots,N-1\\ 1\end{cases}$$

$$\alpha_v=\begin{cases}\frac{1}{\sqrt{2}} & v=0, v=1,2,\ldots,N-1\\ 1\end{cases}$$

The image is reorganized by employing opposite DCT application according to the given equation:

$$x(m,n)=\sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}\alpha_u\alpha_v y(u,v)\cos\frac{(2m+1)u\Pi}{2M}\cos\frac{(2n+1)v\Pi}{2N} \quad (2)$$

A hybrid DWT-DCT approach watermarking domain for the utilization of the mother wavelet, the legibility and imperceptibility of the abstracted/introduced watermark and the image feature indicator for every wavelet family. The host image is disintegrated into four sub-bands and the sub-band LH2/HL2 is selected which employ DWT to every single sub-band and introduce individual watermark value in these sub-bands. In one of the research works (Kumar *et al.*, 2012), the introduction mechanism in the Horizontal (HL) deliver efficient outcome then the vertical sub-band (LH). In another research study (Shefali *et al.*, 2008; Mohamed and El-Mohandes, 2012) researchers employed orthogonal two-fold realm of DCT and DWT alteration and utilized the image characteristics to organize the watermark but the clipping and circulation create maximum disintegration. Furthermore (Lim, 2015; Migdadi *et al.*, 2015) utilized a tremendous frequency to the introduced watermark image dependent on DCT-DWT. The outcome delivered efficient capacity for some ordinary image processing applications.

MATERIALS AND METHODS

The grey scale watermark image with possessing the dimensions 50×20 will be hidden inside a grey scale cover image with dimensions 512×512 with the watermark image, that is the message is the wavelet. Haar level 2 is condensed and then it is introduced in the bits of the cover image. The watermark image is the altered wavelet Haar level 2. The distinct coefficients of the altered wavelet are counted into 3 bits each where there are actually 8 bits. At the same time, the grey scale watermark image may be concealed inside the points of the original cover image. The introduced action is done by concealing a piece of a sector where concealing every section of the grey scale watermark image inside the cover image sector is done (Mohamed and El-Mohandes, 2012; Lal *et al.*, 2015).

Figure 1 displays the flowchart of the complete methodology used in this study. On the left side it displays the watermark infusion and on the right side watermark abstraction after employing the intrusion adjacent to the watermarked image.

Algorithm

Algorithm 1: The proposed algorithm for the introduction of watermark has been displayed in the Fig. 1 with the comprehensive explanation as follows:

Step 1: DWT is utilized to partition the grey scale cover image into four orthogonal multi- determined sub bands: LL1, HL1, LH1 and HH1. LH1 is selected for the later step. DWT isolates an image into under determined matching image (LL) and horizontal (HL), vertical (LH) and diagonal (HH) categories.

Step 2: DWT is once again utilized to partition the sub bad LH1 and acquire minor four sub bands at lower stage and by selecting LH2 sub band. It is vital to observe that another sub band can be selected advancing to various outcomes.

Step 3: LH2 is partitioned into 4×4 regions.

Step 4: Considering DWT-DCT algorithm, DCT is utilized at each region in the appointed sub band. Step 5: Watermark is constructed into units and zeros. Step 6: Pair of distinct un-correlated series are produced. The initial series has been utilized to introduce the watermark bit 0 (PN_0) and the other series has been utilized to introduce the watermark bit 1 (PN_1). Total components in every paired pseudorandom series must be identical to the total mid band components of the DCT altered partitions.

Step 7: Pair produced un-correlated pseudorandom series, PN_0 and PN_1 are joined with the support of progressed determinant k, in the DCT altered 4x4 regions that has been the applicants from the DWT sub-bands of the grey scale cover image. Introduction mechanism is observed in the centre of the DCT coefficients. If it is considered that D is the matrix in the centre of DCT coefficients, then the concealed action can be displayed as:

If watermark bit is 0 then:

$$D' = D+k*PN\_0 \quad (3)$$

where k is a key

Else,

If watermark bit is 1 then:

$$D' = D+k*PN\_1 \quad (4)$$

Step 8: By employing converse DCT and DWT, the watermarked image is re-organized

Watermark extraction: The ownership can be identified from the actual image when some power demands the abstraction of the watermark image and search the real

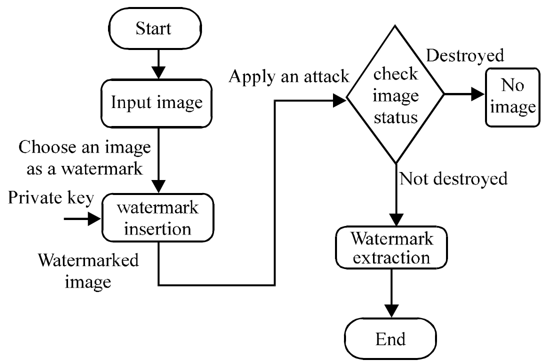

Fig. 1: Methodology flowcharts

owner of the image. In this condition we demand the utilization of the wavelet transform mechanism for instance, DWT and DWT-DCT. The mechanism can be utilized to abstract the watermark as:

Algorithm 2:

Step 1: The assaulted image is further disintegrated into four orthogonal multi determinant sub bands that is LL1, HL1, LH1 and HH1 by employing DWT.
Step 2: After employing DWT one more time to LH1 so as to collect limited four sub bands than the initial one and select the sub band LH2.
Step 3: LH2 is further partitioned into 4x4 regions.
Step 4: DCT alteration is executed in every region in the sub-band LH2 and abstracting the centred band coefficients of each region.
Step 5: Un-identical paired uncorrelated pseudorandom series are produced one more time. Total number of components in every paired pseudorandom series must be same to the number of mid-band components of the DCT altered DWT sub bands. Reproducing the paired pseudorandom series, PN_0 and PN_1 are utilized using the same source that was utilized in the introduction of the watermark mechanism initially.
Step 6: For every region in sub band LH2, the correlation in the middle of the centred-band coefficients and the pair produced pseudorandom series, PN_1 and PN_0 is determined. If the correlation with the PN_0 is advanced than the correlation with PN_1 then the abstracted watermark bit is regarded as 0 else 1.
Step 7: Retrieving the watermark by the utilization of the abstracted bits and calculating the strength of the algorithm by evaluating the correlation amid actual watermark and the abstracted one.

RESULTS AND DISCUSSION

The imperceptibility and robustness watermarking: The proposed algorithm has been employed on 512×512 cover image. After that it has been employed on 50×20 grey scale image with the 'copyright' watermark written inside. It will be displayed that the algorithm is powerful against intrusions such as Gaussian sound, circulation, abridgement which are not very often utilized in real life but are classic and typical. Some of the intrusions such as Gaussian sound are disgraceful while others such as cropping are biased numerical intrusions. Still some others are watermark elimination which aids to measure the correlation between the actual grey scale watermark and the abstracted grey scale watermark from the invaded grey scale cover image. Using the operation, PSNR can be measured as:

$$PSNR = 10.\log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (5)$$

$$PSNR = 20\cdot\log_{10}\left(\frac{MAX_I \text{ pixel value}}{\sqrt{MSE}}\right)$$

Where the Mean Square Error (MSE) is the aggregate squared error amid the altered and the actual image. PSNR is a measure of the peak error whereas MAX is the value of highest pixel. Correlation ρ can be acquired as:

$$P\left(\hat{W}\right) = \frac{\sum_{i=1}^{N} i\hat{w}i}{\sqrt{\sum_{i=1}^{N} {}_{i}^{2}}\sqrt{\sum_{i=1}^{N} \hat{w}_{i}^{2}}} \quad (6)$$

Where ρ is the correlation of the introduced watermark w and abstracted watermark w and N is the measure of the watermark image. By using DWT- DCT transform, the algorithm recorded a better value of PSNR comparing with DWT only. The capability of an algorithm of storing the cover image non-fuzzy is acknowledged as imperceptibility of the algorithm measured by the utilization of peak signal to noise ratio (PSNR). Figure 2 displays the actual image, watermark and the original image plus watermark using DWT-DCT.

After frequent repetitions, the algorithm displays efficient strength across this type of intrusion. Attack factor signifies the extent to which the attack occurs or else it indicates the extent to which the attack affects the watermark image. Correlation signifies the correlation of the watermark initialli, in the very beginning when the outbreak is launched and afterwards thus, analyzing the strength of the algorithm. Correlation operation measures the correlation value in comparison with the threshold value. Utilizing the threshold value, image is regarded watermarked if the correlation value transcends threshold value. From Table 1 and the analysis for the result in Fig. 2 show the results, correlation values of embeded and extracted watermark show clearly that the performance of DWT_DCT is better than DWT against Gaussian noise. On the other hand, correlation values of the rotation attack shows great degradation. This degradation is not due to the lack of capability of the

Fig. 2: The imperceptibility images for original image + watermark by using DWT-DCT

Table 1: Displays the outcome for robustness analysis of DWT-DCT algorithm

Type of attacks	Attacks factor	Correlation (Leena)	Correlation (Papper)	Correlation (Man)	Extracted watermark using DWT-DCT
Gaussian filtter	1.0	0.7300	0.730	1.000	
	2.0	0.7100	0.707	0.990	
	3.0	0.7090	0.700	0.980	
	5.0	0.7060	0.690	0.580	
Gaussian noise	0.1	0.7300	0.700	0.100	
	0.3	0.6500	0.690	0.920	
	0.5	0.6400	0.450	0.570	
	0.7	0.3500	0.400	0.410	
Rotation	35.0	-0.0140	0.026	0.045	
	60.0	-0.0200	0.011	0.036	

Table 1: Continue

Type of attacks	Attacks factor	Correlation (Leena)	Correlation (Papper)	Correlation (Man)	Extracted watermark using DWT-DCT
	90.0	-0.0200	0.006	-0.090	
	180.0	-0.0200	-0.024	-0.030	
Median filtter	1.0	0.7300	0.730	0.980	
	2.0	0.2900	0.260	0.520	
	3.0	0.2200	0.210	0.490	
	5.0	0.0160	0.070	0.170	
Gaussian noise	0.1	0.7000	0.600	0.900	
	0.2	0.7000	0.510	0.720	
	0.3	0.6400	0.310	0.490	
	0.5	0.5200	0.150	0.270	
Rotation	1.0	0.0100	0.030	0.020	
	2.0	0.0060	0.026	0.025	
	3.0	-0.0060	-0.040	-0.090	
	5.0	-0.0200	-0.034	-0.017	

algorithm but comes from the fact that the watermark values has been moved due to the change of the values position through rotation nature. DWT-DCT algorithm breakdown the frequencies into high and low frequency and considers the medium image frequency. DWT-DCT encompasses the criterion that frequency transform is used on a large scale in image compression. Table 1 displays the outcome for powerful analysis of DWT-DCT algorithm counter to Gaussian sound intrusion. Delivered outcome displays better advancement correlation of abstracted and introduced watermarks in comparison with DWT.

CONCLUSION

Through the utilization of DWT and DWT-DCT the powerful digital image watermark technique has been employed with the huge capability of watermark information of actual image. The constructed algorithm is associated with the watermark and by the utilization of DWT and DWT-DCT to maintain ownership privilege by concealing ownership image in another image and safeguard it. Introduction and the abstraction by the utilization of DWT-DCT is efficient than introducing by the utilization of DWT because DWT-DCT breakdown borderline densities. Medium densities of images are considered and DWT-DCT incorporate the reality that the altered frequency is utilized on a large scale in image compression. Watermark image can be abstracted when employing various types of intrusions. Hence, the application of the wavelet classification and execution of Haar transform are effective in sightless and invisible watermark. Assessment of the proposed algorithm, correlation values of the introduced and the abstracted watermark apparently display the efficiency of digital wavelet transform adjacent to dithering. In comparison, correlation values of circulation intrusion display distinct detereoration which does not take place due to the deficiency of the ability of the algorithm bu due to the modifying atitude of the watermark values. The future work, Harmony search and Bat algorithm are examples of Nature Inspired Algorithm that at the moment have not been applied to the optimization of digital image watermarking techniques.

ACKNOWLEDGEMENTS

The researchers wish to thank Universiti Kebangsaan Malaysia (UKM) and Ministry of Higher Education, Malaysia for supporting this work by research grants DIP-2014-018 and FRGS/1/2014/ICT07/UKM/02/2.

REFERENCE

Cox, I.J., J. Kilian, F.T. Leighton and T. Shamoon, 1997. Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process., 6: 1673-1687.

Dharwadkar, N.V. and B.B. Amberker, 2010. Watermarking scheme for color images using wavelet transform based texture properties and secret sharing. Intl. J. Signal Process., 6: 93-100.

Gupta, P.K. and S.K. Shrivastava, 2010. Improved RST-attacks resilient image watermarking based on joint SVD-DCT. Proceedings of the 2010 International Conference on Computer and Communication Technology (ICCCT), September 17-19, 2010, IEEE, New York, USA., ISBN:978-1-4244-9033-2, pp: 46-51.

Kumar, S., A.K. Saini and P. Kumar, 2012. Svd based robust digital image watermarking using discrete wavelet transform. Intl. J. Comput. Appl., 45: 7-11.

Lal, A.M., S.M. Anouncia and O.H. Kombo, 2015. A hybrid approach for fusion combining SWT and sparse representation in multispectral images. Indian J. Sci. Technol., Vol. 8,

Li, Q., C. Yuan and Y.Z. Zhong, 2007. Adaptive DWT-SVD domain image watermarking using human visual model. Proceedings of the 9th International Conference on Advanced Communication Technology, February 12-14, 2007, IEEE, New York, USA., ISBN:978-89-5519-131-8, pp: 1947-1951.

Lim, H.I., 2015. A performance comparison on characteristics of static and dynamic software watermarking methods. Indian J. Sci. Technol., Vol. 8,

Migdadi, H.S.O., H. Obeidat, K.O. Anoh, N.N. Khatib and J.M. Noras et al., 2015. Channel estimation for OFDM FFT/DWT in multi-carrier modulation used in wireless telemedicine. Proceedings of the 2015 IEEE International Conference on Computer and Information Technology: Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), October 26-28, 2015, IEEE, New York, USA., ISBN:978-1-5090-0154-5, pp: 1057-1062.

Mishra, A., C. Agarwal, A. Sharma and P. Bedi, 2014. Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm. Expert Syst. Applic., 41: 7858-7867.

Mohamed, M.A. and A.M. El-Mohandes, 2012. Hybrid DCT-DWT watermarking and IDEA encryption of internet contents. Intl. J. Comput. Sci. Issues, Vol. 9,

Shefali, S., S.M. Deshpande and S.G. Tamhankar, 2008. Attack detection through image adaptive self embedding watermarking. Intl. J. Signal Process., 4: 260-266.

Shensa, M.J., 1992. The discrete wavelet transform: Wedding the a trous and Mallat algorithms. IEEE. Trans. Signal Process., 40: 2464-2482.

Waleed, J., H.D. Jun, T. Abbas, S. Hameed and H. Hatem, 2014. A survey of digital image watermarking optimization based on Nature Inspired Algorithms NIAs. Intl. J. Secur. Appl., 8: 315-334.

Zhang, X., S. Wang, Z. Qian and G. Feng, 2011. Reference sharing mechanism for watermark self-embedding. IEEE. Trans. Image Process., 20: 485-495.