Evaluating Digital Image Watermarking based on Image Interlacing, DWT & DCT.

Mahejabi Khan  
Dept. Computer Sc. & Engg.  
Rungta College of Engineering & Technology, Bhilai, India.

Ajay Kushwaha  
Dept. Computer Sc. & Engg.  
Rungta College of Engineering & Technology, Bhilai, India.

Toran Verma  
Dept. Computer Sc. & Engg.  
Rungta College of Engineering & Technology, Bhilai, India.

Abstract—Digital watermarking is important as it facilitates security & protection to digital data whereas when this data are used within international network they must exist in compressed format as it requires minimum transmission bandwidth & reduced storage requirement. Hence our proposed scheme will serve as a solution for maintaining the digital data in compressed state. To achieve this goal the procedure will perform watermarking of interlaced image based on DWT – DCT algorithm. In order to embed the watermark we transform the image into subimages using 2-level interlacing, then the selected subimage is 1-level decomposed using DWT haar wavelet transform, from the decomposition the sub-image is selected which is also transform by DCT algorithm. Hence the watermarked image is formed by inverse transform of DCT followed by IDWT.

Watermark Embedding & Watermark Extraction are the two important component of any watermarking system.

The “Watermark Embedding” is the process of inserting the secret information (noted as watermark) into the host signal and the image thus produced after embedding becomes “watermarked image”. This watermarked image is then transmitted into the network and at receiver end the “Watermark Extraction” algorithm which being the inverse of watermark embedding procedure is applied over the received signal in order to retrieve watermark. The extraction process must be robust against various attacks [3, 15].

An efficient watermarking system should satisfy the two requirements. Firstly, the presence of watermark must be imperceptible for human eyes and should not degrade the quality of the original media visually. Secondly, the watermark should be robust & able to survive when data signal are exposed to attacks over noisy communication channel and any unauthorized party must not be able to remove the watermark [15]. MSE, SNR, PSNR, BER, NC are the quality metrics for measuring the performance of watermarking system [21].

Based on the embedding & extraction procedure, the digital watermarking can be classified into various categories i.e. according to domain, host media, watermark & requirement of the original host media to extract the watermark. These classification is illustrated in figure below:

Fig. 1(a). Classification of digital watermarking.
1) Based on Domain:
In spatial domain the coefficient of original image is directly used whereas in the frequency domain the original image is transformed to obtain its synonymous transformed-domain image and the coefficients of this image are modified in order to embed the watermark [2, 22]. This technique is effective and efficient than spatial domain because it yields more information embedding capacity, good perceptual transparency, compatible with image compression standards, offers robust watermarking and is resistance against many attacks because the watermark is scattered over the entire image which makes difficult for intruders to interpret the watermark, but imposes complex implementation and higher computational cost [15, 18, 22, 23]. The most commonly used algorithm to transform the coefficient of an image are Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) etc. [4, 12].

Apart from the above two domain, the blend domain is also developed which utilizes the beneficial feature of spatial & transform domain simultaneously [2].

2) Based on Host media:
With text watermarking, the watermark is inserted in line space, between character’s space & font shape. When image watermarking is considered it adds the watermark into the image. Whereas with audio watermarking audio file is used for embedding, video stream is used when video watermarking is done and when watermark is embedded into 2D/3D computerized graphics is termed as graphics watermarking. [23].

3) Based on Watermark:
Based on application of watermark - Source based watermarking is exploited for ownership identification whereas Destination based watermarking is used for recognizing of particular distributor or recipient [24, 31].

Based on number of watermark to be embedded - Single watermarking embeds single watermark whereas multiple watermarking embeds multiple watermark into a single digital data [19].

On basis of Human Perception – In visible watermarking watermark is perceived visually whereas in Invisible watermarking the watermark is kept hidden into the cover image i.e. not visually observed. Its advantage is to enhance the imperceptible feature of watermarked image and can only be detected by an intelligent system [2, 10, 25].

Also based on permanency, invisible watermarking is classified into three types: Robust, Fragile, Semi fragile watermarking. Amongst which robust watermarking is exploited & this is designed to resist against intentional/unintentional attacks which is basically concerned with copyright protection, copy control, fingerprinting and broadcast monitoring [2, 21, 25]. On the other hand, fragile watermarking is used to recognize any unauthorized manipulation[10,21] and the semi-fragile watermarking are designed for recognizing any unauthorized modifications and at the same time it is robust against incidental modification (e.g. image processing attack) [21].

4) Based on watermark extraction procedure:
Non blind require the original cover image, blind watermarking does not require it whereas semi-blind does not require the original image but need the watermark or its additional information only for retrieval of exact watermark [2, 12, 18].

This paper is organized as follows: Section II describes the preliminary concepts, and on basis of the concepts Section III discusses the literature review, Section IV contains the proposed methodology, section V holds the results, conclusion and future scope is given in section VI.

II. PRELIMINARY CONCEPTS

2.1 Image composition & Transformation coefficient importance in watermarking:
Mostly the realistic image is a composition of sharp variant & smooth variant where sharp variant (fine detail such as texture, edges etc) lies in between the smooth variant (image base such as flat regions, slow varying regions, color etc). Technically, low frequency components (LL) are represented by smooth variations & high frequency components (HH) are indicated by sharp variations [5, 7]. Any image processing operation is performed after the separation of these components. Since, the low frequency components of image at the edges do not describe the signal fairly, so some energy from low frequency part leaks into high frequency parts which give rise to middle frequency components (HL, LH) [7]. The low frequency components constitute with most important image information and any alterations (adding of watermark) will degrade the quality of host image but imparts robustness. The high frequency components consists of least important image information (such as edges, texture), imperceptibility will be achieved if this region is used for watermarking but watermark will be eliminated when the image is exposed to image processing operations (say compression) . The best portion for watermarking is Mid frequency components (horizontal, vertical details) because it offers tradeoff between imperceptibility & robustness. According to characteristics of HVS model, the vertical components are more sensitive to human eyes than horizontal components. Hence the watermark will be more imperceptible when embedded in the horizontal detail of middle frequency component [4, 12, 19, 20].

2.2 Discrete Cosine Transform(DCT): Transformation using DCT tends to minimizes the information by removing the redundant data of the media [4,16]. DCT is a widely used scheme for image transformation which imparts various advantages such as good information packing ability and low calculation complexity, high resistive to image processing attacks,
compression attack etc. It also provides suitable trade-off between HVS model and the image deformation degree [29, 30, 31]. Global DCT watermarking and Block-based DCT watermarking are the two variants of DCT watermarking. DCT computation is performed on the entire image or on the non-overlapping blocks to obtain lowest frequency(FL), middle frequency(FM) and highest frequency(FH) components[1,5,16,31]. According to [3], for a image of size N*N DCT is defined in equation 1,2,3 & 4.

\[
f_{fl}(u,v) = \frac{1}{N} \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} \phi_{ij}(m,n) \cdot f(m,n) \cdot e^{-j2\pi(mu+Nv)} \\
f_{fh}(u,v) = \frac{1}{N} \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} \phi_{ij}(m,n) \cdot f(m,n) \cdot e^{j2\pi(mu+Nv)} \\
\]  

where: \(f_{\text{fl}}(u,v)\) represents 2D-DCT, \(f_{\text{fl}}(u,v)\) represents 2D-IDCT & \(N\) is number of pixels in \(u\) rows & \(v\) columns i.e. \(N = 4,8,16\) etc.

2.3 Discrete Wavelet Transform(DWT): Using this transform the coefficients to be watermarked can easily be identified because it is analogous to the HVS model & understands it more precisely [4]. DWT based watermarking offers following advantages such as a large watermark embedding capacity, good robustness against noise, good energy compaction properties which leads to effective data compression [7, 27]. Wavelet transform implementation can be accomplished using various digital filters such as Haar, Symlets, Daubechies etc [11]. The basic idea behind wavelet transform for processing the image is its multi-resolution decomposition which decomposes the image into sub-images of different frequencies (such as low frequency & high frequency) with different resolutions [1, 2, 15, 19, 27]. As DWT analyze the signal in both spatial & frequency domain [8, 17, 27, 30], this spatial-frequency (time-frequency) representation locate the low frequency components in frequency domain & the high frequency components in spatial/time domain precisely [22]. The first decomposition level is resulted after the horizontal & then vertical filtering (or vice-versa) of image which decomposes the image into four subbands i.e. one approximation (low frequency or coarse wavelet) coefficient and three detailed (high frequency or finest wavelet) coefficient i.e. LL (approximation) and high frequency coefficient is labeled with HL (Horizontal Detail), LH (Vertical Detail), HH (Diagonal Detail) [3, 12, 13, 19, 20, 21, 22].

The multi-resolution capability of the transform offers scalability i.e. to obtain the next decomposition step to obtain LL subband is further decomposed into four subbands and the process continues until the desired DWT decomposition level is reached [7, 13, 15, 20, 24]. More decomposition level means lesser frequency subband resolution with higher important coefficients while the other detailed bands can be classified of lesser importance [5, 27]. Generally for watermarking or compression application decomposition are done not more than up to four levels[3] because watermark embedding capacity will decrease [14, 48] on the other hand more decomposition leads to ringing artifacts around the edges [7]. According to [8], For image \(f(x,y)\) of size \(M \times N\) the DWT is given in equation 5 & equation 6.

\[
W_L(j0,m,n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cdot \phi_{j0,m,n}(x,y) \\
W_H(j,m,n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cdot \psi_{j,m,n}(x,y) 
\]  

where \(W_L(j0,m,n)\) is low frequency component & \(W_H(j,m,n)\) is defined as horizontal, vertical, diagonal details of \(f(x,y)\), \(i=\{\text{Horizontal, vertical, diagonal}\}\), \(j0\) is arbitrary scaling factor where \(j \geq j0\).

III. LITERATURE REVIEW

Our research work is based on image interlacing followed by watermarking using combined DWT-DCT algorithm as these are amongst the transform methods which are mostly used in image processing applications. Some previous researches are described below which forms the foundation of our research work.

LITERATURES from which the concept of interlacing is studied:

B. Sridhar et al.[10] utilizes interlacing approach for multiple watermarking system, author interface the original image into two sub images. Hence one sub-image per watermark will be used for multiple watermarking concept. Following this forward & reverse 1-level DWT is performed where ever required for watermark embedding and its extraction. The results achieve excellent robustness against many geometrical attacks. From the paper it is also concluded that the subimages are very similar to each other which forms the idea for [12] paper.

Mohamed M. Ibrahim et al.[12] proposed image interlacing as a new technique in non-blind image watermarking system for color image is proposed which utilizes the n-level interlacing approach (where \(n = 1,2\)) to produce the sub-images. Hence during extraction these sub images plays the similar role of those identical copy of host image which are required in ordinary non-blind watermarking approach. From the selected pair one is picked which is DWT decomposed by 3-level followed by embedding of watermark(there encrypted image) to produce watermarked image. The scheme proves its robustness against various attacks without any performance drop.

www.ijcsit.com 13
Literature that based on hybrid DWT-DCT algorithm is discussed below in which:

1) DWT is widely used for identifying the watermarking coefficient (sub band).
2) Watermark and / or selected coefficient are DCT processed for embedding of watermark.

Keta Raval et al.[3] also utilizes hybrid DWT-DCT scheme for watermarking, along with watermarking the scheme also provides the way to do secure transmission of data over network against attacks. As efficient data transmission requires minimum storage space, less bandwidth requirement so the watermarked data is first compressed before transmission over network. During transmission inorder to overcome the effect of attacks on the data and to receive the data error free error correcting code is applied. The performance of the scheme is tested against various attacks and tends to be robust against attacks & noises over communication channel.

Afroja Akter et al.[6] proposed hybrid DWT-DCT algorithm for watermarking which utilizes the DWT transform for decomposing the cover image by 2 level, 3 level, 4 level followed by DCT transform on processed image as well as on watermark information. The performance of this paper is compared with Cox’s additive algorithm for AWGN attack & without attack to provide better results over Cox’s algorithm in terms of good PSNR, better extraction & embedding of large sized watermark.

Yang Qianli et al.[9] proposed composite watermarking algorithm based on DWT-DCT for gray scale image. From this literature the implementation of hybrid algorithm is studied, on host image DWT is applied for 3 level to split the images into sub blocks and DCT is applied on the selected sub blocks as well as on the watermark to produce DCT coefficients. The DCT coefficients of sub blocks are sorted in decreasing order and the maximum coefficients are selected for embedding the watermark sequence. Finally, for extraction of watermark the reverse of the two transform is applied. The result of watermarking using this hybrid scheme shows that the approach is robust against common signal processing attacks ( JPEG compression, noise etc.)

Literature for embedding of watermark sequence into the host image using DCT is given below:

Saeed Al-Mansoori et al.[26] proposed blind & robust image watermarking algorithm based on DCT odd/Even technique to embed watermark (logo) into cover image (DubaSat-1 satellite image) for the purpose of ownership protection. In this paper from the cover image the best location of the low frequency component of each (8*8) DCT blocks is selected for embedding the watermark with a secret key (location of the highest magnitude of first 16 lower frequency coefficients). The author proposed three different methods namely 1(A), 1(B), 1(C) for watermarking where 1(A) embeds single watermark image, 1(B) embeds two watermark image redundantly & 1(C) embeds three watermark images redundantly and each method is tested against flipping, noise, resize and rotation attacks. The conclusion of the paper says the method 1(A) is yields highest PSNR, robust against noise and flipping attacks. Method 1 (B) results robustness against rotation & resize attacks whereas the result of method 1(C) gives lesser PSNR.

Blossom Kaur et al.[28] proposed blind & moderate robust watermarking based on DCT domain which provides good resistance to common image processing attacks. The watermark is embedded into the middle frequency DCT coefficient using the watermark sequence (watermark converted into binary sequence) and the pseudo random number sequence. From the future scope of the paper it is studied that DCT algorithm can be combined with DWT for security purpose & when combined with SVD imparts strong robustness as the combination of the two algorithms will compensate the fitfalls of each other.

Okkyung Choi et al.[32] proposed DCT domain watermarking for image integrity verification. This watermarking approach intended to recovery the image by image reverse conversion process and the recovery rate of watermark is enhanced by embedding the watermark image into the cover image redundantly & dispersively. Experimental results show that the watermarking approach is highly robust to geometric attacks.

Based on the advantages of hybrid algorithm of DWT-DCT which results to be robust against attacks such as compression, noise etc as shown in paper [3, 6, 9]. Our proposed idea is to modify the paper [12] by utilizing the combined DWT-DCT watermarking approach. In our methodology the host image (color image) is interleaved using DWT, the level of interleaving and DWT depends on the size of the watermark(which is a message) to be embedded. Also the level of interleaving must be even because it will result into sub images of square matrix which will be required when it is processed by block based DCT. After performing DWT the selected area is 8*8 DCT transformed with the aim to impart imperceptibility and robustness to the watermark.

IV. PROPOSED METHODOLOGY.

Watermark embedding & extraction algorithm:

Step 1. Read the cover image.

Step 2. Interlace the image, proceed with 2-level interlacing because its decomposition will result into square matrix and this will be required during DCT based embedding step.

Step 3. On the selected sub-image apply 1-level DWT and select its HL component for watermarking. All three component say RGB of the above selected sub-image will be used during processing.

Step 4. Read the watermark text, convert it into binary sequence.

Step 5. On the above selected subimage, apply 8*8 DCT and select its mid frequency coefficient for embedding of watermark.

Step 6. Apply inverse DCT followed by inverse DWT in order to obtain the watermarked image. The watermarked image obtained in this step is the interlaced image which is processed for watermarking.

Step 7. Apply DWT followed by DCT on the watermarked image in order to dether the image and extract the watermark.
Watermark embedding & extraction operation.

Embedding: $I_w(x,y) = I(x,y) + k * w$

where $k = \{-k \text{ for } w=1, +k \text{ for } w=0\}$

Extraction: if $(I_w(x,y) > 0)$

\[ w = 0; \]

else

\[ w = 1; \]

Where: $I_w(x,y) =$ watermarked image coefficient.

$I(x,y) =$ original image coefficient.

$k =$ random number.

$w =$ watermarked bit.

V. RESULT

For simulation of the proposed algorithm MATLAB (R2013a) software is used. Using standard image database various test images have been taken. In our experiment the cover image is the color image of size 512*512 and watermark is the text (maximum of 32 characters). We have tested on “F-16” image with “mahejabi from rcet” as watermark. The test results are illustrated in figure below:

Fig.5(a). watermark recovery without attack; MSE = 0.004, PSNR = 72.04 and BER = 0.02

Fig.5(b). watermarked image with rotation attack; MSE = 0.18, PSNR = 55.45 and BER = 0.52

Fig.5(c). watermarked image with laplacian attack; MSE = 0.29, PSNR = 53.40 and BER = 1

Fig.5(d). watermarked image with blurring attack; MSE = 0.07, PSNR = 59.65 and BER = 0.42

Fig.5(e). watermarked image with brightening attack; MSE = 0.18, PSNR = 55.40 and BER = 0.40
The performance of the proposed algorithm is evaluated using measures such as MSE, PSNR in order to find the degradation of the original image vs embedded image & original image vs attacked image. Also BER is used to determine the error received in bits of the extracted watermark. The above performance index is formulated as:

1) The Mean Square Error (MSE) is defined as average squared difference between the original cover image and watermarked image. If MSE increases watermarked image quality gets decrease. Ideally, for a good algorithm should reach to zero. For an NxN image it is calculated by the formula given below [9, 33]:

\[ \text{MSE} = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} (X(i,j) - X'(i,j))^2 \]

Here X(i,j) is original pixel value and X'(i,j) is decoded pixel value.

2) The Peak Signal to Noise Ratio (PSNR) measures the degradation in the watermarked image with respect to the cover image. It is widely used metrics to measure imperceptibility. In ideal case when PSNR reaches to infinity, watermarked image thus produced is of the higher quality. Higher PSNR indicates less difference between the two corresponding image. It is calculated by the formula given below [2, 9, 33]:

\[ \text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}} \]

3) The Bit Error Ratio (BER) is the ratio which determines the number of received bits in error with respect to the total received bits when transmitted over noisy channel.

\[ \text{BER} = \frac{P}{(H \times W)} \]

Here H is height & W is width of watermarked image. P is a counter set to 0 & is incremented by 1, if there exist bit difference between cover image & watermarked image [33].

VI. CONCLUSION & FUTURE SCOPE

In this paper, we proposed the hybrid "Interlacing-DWT-DCT" watermarking scheme with the aim of keeping the cover image in reduced sized format which will be required during ownership authentication. The results of the proposed watermarking technique do not seem to be robust against attacks and results in higher manipulation of the watermark text after extraction. So in near future we will try to enhance the performance of the proposed hybrid algorithm using different strategies for embedding & extraction of watermark inorder to impart better robustness to the scheme.
REFERENCES


[26] Saeed AL-Mansoori, Alavi Kunhu, "Robust Watermarking Technique based on to protect the ownership of DubaiSat-1 images against attacks",IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.6, June 2012.


