Digital Video Watermarking Scheme using wavelets with MATLAB

Deepak Chaudhary
Assistant professor
Computer Science Engineering Department

Prachi Sharma
M. Tech Scholar
Computer Science Engineering Department

ABSTRACT
With the extensive use of Internet, transfer or sharing of digital data online is enormous. This leads to easy accessibility and vulnerability to attacks of copyrighted content on large scale. Digital multimedia in the form of videos, audios, text, images or digital documents can easily be manipulated, forged and redistributed for profits. To overcome this problem and protect copyrighted content, Digital Watermarking emerged as a useful solution. The project work is based on two main viewpoints. The first viewpoint describes about the different watermarking techniques and showcases the comparative description of superiority of one technique over the other. It is seen that frequency domain is more suitable domain for watermarking schemes as it yields robust results as compared to other domains such as spatial domain.

Keywords
MATLAB, Wavlet

1. INTRODUCTION
Internet environment is open for all. With the widespread use of internet facility, anyone can have easy access to digitized multimedia such as videos, audios, documents and images. Internet downloading is also easily achievable. But this give rise to problems in copyright protection as it enhances illegal copying, and distribution of copyright content at large. Digitized content in the form of images, audios, text, files and videos can be easily copied, moved, modified, redistributed which can also be referred to as Forgery of data. This is huge threat to copyright owners as their work gets manipulated and distributed. This leads to decline in their profitability. Also, anyone can claim its authority and ownership if the information about the actual owner of data is missing. Hence, to overcome such copyright and intellectual right protection issues, Digital Watermarking emerged as a useful solution [1].

Digital Watermarking (shown in Figure 1.) is different from the techniques of Cryptographic encryption/decryption as the data in encrypted form becomes non-readable and will not be of any use if users desire to view that data. Through the technique tim data, numerical data, audio signals, images or can be signatures.
A watermarking scheme is expected to possess three main characteristics:

1. High Fidelity,
2. Good Robustness, and,
3. High Data Capacity [3].

Fidelity implies that the watermarked image should be as perceptually equal as possible to the original host image. Withstanding several processing attacks, yet the information stored inside the watermark remains intact and can be extracted successfully, leads to its robustness. The more the capacity, more private information can be embedded inside the original host image.

However, it is difficult to achieve all characteristics in one watermarking scheme as focusing on fidelity may lead to decrease in robustness, or striving to store more information inside the image may hamper the image quality. Watermarks must be embedded in the host content in such a manner that it becomes difficult to remove and perceive [4].

2. TRANSFORM DOMAIN
In frequency domain, transform coefficients are adjusted for watermark embedding. It is used widely as compared to spatial domain as it yields more robust results to geometrical transformations such as translation, scaling, bending, shearing, rotation [4] and compressions [1]. It also helps maintain the imperceptibility of original host image. Common transforms used for watermarking are, discrete Fourier transform, discrete cosine transform, discrete wavelet transform, wavelet packet transform, principle component analysis which is a linear transform. These transforms are described in detail in further section.

Table 1. Comparison between spatial domain and frequency domain [6]

S.No	Spatial Domain	Frequency Domain
1	Simple technique to use by modifying pixel values	Complex to use by modifying transform coefficients
2	Lack Imperceptibility	High imperceptibility
3	Less robust, incompetence in dealing with a range of attacks	More robust against different types of attacks
4	Restricted capacity of an image to hold the watermark	High capacity to hold watermark
5	Involves less computational cost	High computational cost involved
6	Poor performance suitable only for video watermarking where video quality is given priority over robustness to attacks.	Better performance and results

3. APPLICATIONS OF WATERMARING

Following are the various watermarking applications used in real life areas [18]:

1. **Copyright protection,** it is probably one of the most commonly used of watermarking application today. Information of copyright owner is embedded in original host image in order to safeguard from claiming ownership of content.

2. **Fingerprinting,** the fingerprint embeds the relevant information about legal recipient in the digital content. This involves embedding distinct watermarks into each of the image and permits the owner to monitor and locate pirated content which is illegally obtained.

3. **Prevention of unauthorized copying** is achieved by embedding the relevant information about how often an image is likely to be legally copied. An ironical example where the exploitation of a watermark might have avoided the wholesale burglary of an image is in the Lena image that has been utilized without the permission of original owner.

4. **Image authentication,** in an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences.

4. LITERATURE SURVEY

Research in the field of Digital Watermarking gained attention in early to mid-1990s. Since then, it has gained wide exposure and many different techniques have been proposed with the common goal to achieve high robustness and imperceptibility facing newer challenges.

In paper "Evelyn Brannock: Watermarking with Wavelets: Simplicity leads to Robustness" [18], Evelyn used Discrete Wavelet Transform (DWT) technique in frequency domain to implement digital watermarks. The watermarking algorithm used a database of many images with their various properties. All the images used are grayscale images. They used Eight different families of wavelets, orthogonal and biorthogonal both and compared them for efficacy. The wavelet families used were: Haar, Daubbechies, Daubbechies32, Symtel, Coiflets4, Bior 2.2, Bior 5.5, Rev. Bior 6.8. To measure the performance and success of the algorithm and the impact of mother wavelet objectively, PSNR value of each wavelet family and the image is calculated. Noise is also added to reproduce and check against various attacks. It is concluded that the performance of simpler wavelet transforms, like, Haar wavelet, is better than the more complex wavelet transforms. The algorithm used 2-dimensional DWT which decomposes the digital image into sub-images. The digital image is thus separated into lower and higher resolution bands. The watermark is then embedded inside the high resolution band as it is less sensitive to human vision thus increasing robustness. The watermark can then be extracted from the watermarked image using the 2-dimensional inverse DWT. The images were tested against three types of noise: Gaussian, salt and pepper and speckled. The experimental result proved that when testing on Embedding watermarks with/without noise, and extracting watermarks with/without noise, Haar wavelet gave better results than other watermarking transforms.

In paper "Salwa A.K Mostafa: Video watermarking scheme based on PCA and wavelet transform", Salwa A.K Mostafa, [16] used binary logo watermarks to embed into video frames by using the concept of linear transform PCA and discrete wavelet transform. The video is divided into video frames and then on each frame DWT is applied to get two frequency bands (LL-HH). Next PCA is applied to provide complete decorrelation among bands thus enabling data hiding. Lastly, binary watermark is inserted into the luminance parts of PCA components of LL and HH blocks. Here 2 different types of transforms are used in order to enhance the performance of the algorithm. In this paper, lowest and highest frequency bands are chosen to apply PCA and to embed watermark. Later to achieve the watermarked image, inverse PCA and inverse DWT is applied. Salwa suggested a non-blind scheme for watermarking. It was observed that after applying discrete wavelet orthogonal decomposition by using discrete wavelet transform, wavelet coefficients still have some correlation among them. Thus, principle component analysis technique is used to remove the correlation completely. PCA also helps in concentrating high energy which further enhances its data hiding capabilities. To perform watermark extraction, the watermarked image and the original referenced image is taken and compared and the watermark is extracted. The experimental outcomes showed that there exists no visible difference between the original and watermarked frames. To check the robustness of the image, wide range of attacks such as MPEG coding, JPEG coding, Gaussian noise addition, contrast adjustment, cropping, resizing, rotation, sharpen filters, scaling, histogram equalization, gamma correction, frame dropping, and frame averaging. are applied. Peak signal to noise ratio is used as a quality parameter to evaluate the performance. PSNR values are obtained and analyzed for the watermarked frames as well as the attacked frames.

Hassen [4], has proposed the use of Schur transformation for the watermarking scheme. Schur transform is a mathematical transform and a new domain for representing images and for embedding watermarks. The method proposed is robust against many attacks both asynchronous attacks such as geometric attacks which can be rotation, scaling, cropping, shearing, translation, change of aspect ratio, and random bending and synchronous attacks such as filtering, noise addition, or compression. The used technique despite showing robust results also lowered down the possibility of error detection. In this, blind watermark is used for embedding, hence, there will be no requirement of the host image for watermark detection and recovery process. The study provides a 2-d variable function which represents the strength of watermark embedding exploited to pass up any distortion of watermarked image. According to the proposed technique, initially, the original image is transformed into schur domain which is represented in form of a triangular matrix. Then, non-sensitive zone is identified by carrying out tests where the watermark can be suitably embedded keeping the image quality unaffected. Lowest values of the matrix are processed so that as lowest distortion on watermarked image is possible. This technique has the advantage that it allows high embedding strength yielding robust results against spatial method or DCT, DFT. It showed high resistance against large set of both asynchronous and synchronous attacks. The watermark was found to be present in the attacked image.

Embedding watermark can be considered as an optimization problem. For a good watermark, robustness capacity and fidelity are the characteristic features that must be satisfied but they all cannot be satisfied together as they conflict with each

other. If fidelity is increased, it may lead to decrease in robustness and data strength. Whereas, if large amount of informative data is inserted, then it may lower down the fidelity of watermarked data. Hence, adopting an optimal scheme is required. With this viewpoint, Yueh-Hong Chen [3], proposed GA based image watermarking technique using wavelet packet transform. Wavelet Packet Transform can be considered as a generalized version of wavelet transform. It allows decompositions to be represented by any of permissible base represented by the subtree. It adopts redundant basis function and provides time-frequency resolution. GA is applied in frequency domain to find out the optimal coefficients that can be manipulated for watermark embedding. Wavelet packet decomposition allows decompositions to be represented by any of permissible base represented by the subtree and with the use of genetic algorithm it allows to select most appropriate base to increase robustness. For embedding watermark, genetic algorithm is being used to find out the optimal base of WPT and random chosen coefficients are being used. Genetic algorithm is applied by selecting the parameters, fitness function and fitness values and having proper mutation and mate ratio to get the optimal value in each iteration of the evaluation while coefficients are being used in the manner if first watermark bit is 1 then all other coefficient should be smaller than first coefficient and if it's 0 then all the coefficients are greater than 0. Extraction of the watermark involves the comparison of the first coefficient with largest and smallest from the remaining coefficients. Experimental results showed that the proposed method can help increase the ability to defy image processing methods if some appropriate GA fitness function is opted.

A hybrid combination of both DWT and PCA is proposed in [15-16]. PCA helps in providing complete decorrelation among coefficients and enhance data hiding. In [15], binary watermarks are embedded in video frames. The host video is first decomposed into sub bands using 3 level DWT, then, after applying entropy to each block, some blocks are selected on which PCA is applied. Then, the watermark is embedded into the highest coefficient values of PCA blocks. The algorithm showed high robustness and high imperceptibility when subjected to several attacks.

Qianli [1], proposed the algorithm for gray scale images based on 2 dimension discrete wavelet image where DWT to multiple level has been applied before applying DCT to achieve watermarking to achieve more imperceptibility and enhanced robustness. Selection of number of levels for decomposition of the original image into discrete level domain serves as basis of the secret key while extracting the watermark. To protect the copyright information of digital media efficiently, initially, the grayscale image is taken as input which is first transformed into discrete wavelet components up to 3 levels to get the decomposed blocks. Then, to each sub block, discrete cosine transform is applied. The watermark image is also transformed into discrete cosine components and thus embedded into the sub blocks of the host image and then inverse of DCT and DWT is applied to get the watermarked image. The Watermark extraction algorithm proposed was the reverse of the embedding process to achieve the watermark. To check quality of the image, subjective as well as objective criteria were analyzed. The experimental results showcased that algorithms applied yielded robust outcome when the watermark was subjected to lossy compressions, low pass filtering, cutting, and noise.

DCT based video watermarking technique for embedding blind watermark is proposed by Nilanjan et al. in [17]. In this, firstly each of the video frames is sub divided into multiple blocks which get to formed using DCT technique. Then the watermark is embedded inside the uncompressed frame components into the luminance parts of the cover data in order to avoid chrominance quality distortion. The secret key is created which can be further used for watermark extraction.

Mohamed in the paper "Robust Method of Digital Image Watermarking using SVD Transform on DWT Coefficients with Optimal Block" [19] formulates the model which is based on the properties of DWT, DCT and SVD for providing the imperceptibility and robustness. In addition to implementation of these transformations, Mohamed includes the selection of the optimal block in terms of maximizing the amount of information to be inserted into the cover image. The embedding process includes DWT decomposition of the cover image into sub bands which is further analyzed to get the entropy of each block to select the optimal block for inserting watermark. Once optimal block has been identified, firstly DCT has been applied to that block and then SVD has been applied on the resultant coefficient matrices. Watermark image is also undergone though DWT first to get sub block so that singular value can be identified of the block which is further use for modifying the singular values obtained from cover image. After modification of the singular values, inverse DCT and DWT has been applied to get the watermark image. PSNR values has been determined against 9 different attacks to measure the performance of the watermarked image which shows that HH and LH are the best coefficients to insert watermark after the selection of the optimal block of maximum capacity.

Mehran [2] proposed the technique of grayscale watermark logo embedding inside the host image using texturization scheme. In this, initially the host image is separated into fairly textured and poorly textured regions. Then, the watermark logo is converted into similar texture using Arnold transform and one lossless rotation technique to map with fairly textured image regions. Whereas, for the poorly textured regions, only lossless rotation is performed on the watermark logo. The watermark is then embedded into the host image regions using wavelet based embedding techniques.

Jeril George proposed watermarking technique by applying DWT, SVD with Arnold transformation [13] where DWT is applied to provide imperceptibility and SVD to give robustness. But DWT and SVD together can't handle the security issues with watermarking and hence George has explored idea of implementing Arnold transformations which ensure that watermark will be available to only authorized user. In this model, original and watermark images first split into RGB channel to act as input for further embedding process. DWT and SVD has been applied on the blue channel of the original image while first Arnold transformation has been applied on blue channel of watermark image which in turn act as key (available to owner and distributor). After Arnold transformation, SVD has applied on watermark image. Singular values obtained from the cover image are modified according to singular value of watermark image to embed the watermark into it whose result will go through inverse DWT and merging of the color schemes to get the watermarked image. The usage of key (obtained in the process of embedding watermark) while extracting the watermark makes this technique as semi blind technique which means there is no need of original image to extract watermark. The technique implements watermarking using level-3 DWT, followed by

SVD of the LH sub band of the cover image and applying SVD to the scrambled watermark. Singular values of the cover image are modified to embed the scrambled logo. Algorithm presented involves semi-blind watermark extraction which avoids the need for original image during extraction process. The watermarking system gives good imperceptibility and robustness against various image processing attacks. Arnold transform is used to cater to the need of watermark security as the intention is that the watermark after extraction should be visible only to the authorized and authenticated users. Hence, a secret key is shared between the owner and intended users. This semi blind technique makes it robust against the attacks and makes it more secure. The quality of the watermark has been measured among various attacks like salt & pepper, guassian noise, mean values, median values, jpeg compression, cropping, histogram equalization; in each of the attack the proposed model has provided the better results when measuring PSNR to check the imperceptibility and correlation Coefficient to check the robustness of the watermarked image.

In paper "Luigi Ros: High capacity Wavelet watermarking using CDMA multilevel codes", [20] Luigi Ros used CDMA and multilevel code technique to implement the watermark. Initially, DWT in frequency domain is applied on the host image which separates it into lower resolution and higher resolution bands (horizontal, vertical and diagonal) sub images. Then, multilevel CDMA algorithm is applied for wavelet based watermarking scheme. This technique gave robust results against attacks such as filtering, cropping and compression.

In paper "Maria Chroni: Watermarking images using 2D representation of self-inverting permutations", [21] spatial domain is used to embed numerical watermarks in digital images. Firstly, the integer watermark is converted into self-inverting permutation using the concept of Bitonic Permutations. Next the watermark is embedded into the host image in spatial domain by modifying the pixel values which are undetected by human vision.

HVS characteristics along with Spread Transform has been proposed in [20] for watermarking scheme. Already known spread based transformations use watermark signal with real number sequences which were not able to have unique signature and hence the use of spread watermark according to Watson Model to convey unique information with great resiliency is proposed in this paper. Watermark image is firstly spatially dispersed and then Hadamard transformation is applied on cover & dispersed watermark image. After sorting out the transform coefficients of the cover and the watermark image in ascending order, apply the modular function obtained from the application of Watson visual and exponential function of entropy masking model and then block based inverse Hadamard transform is applied to form watermarked image. This scheme is showing resiliency even after embedding of watermark multiple times to the original image.

Watermark Embedding Algorithm

The embedding procedure involves various steps as mentioned below and represented as in figure.

Step1: Read the host video and divide the video into frames.
Step2: Split each of the frame into Red, Green and Blue components.
Step3: Convert the RGB components of each of the frames into Grey components.
Step4: Apply random number generator to select random set of frames for watermark embedding.
Step5: Apply discrete wavelet transformation using db wavelets to each of the randomly selected frames in order to obtain four frequency sub bands, LL1, HL1, LH1 and HH1.
Step6: Now take the LL1 frequency sub band and apply second level DWT to obtain LL2, HL2, LH2 and HH2.
Step7: Again take LL2 frequency sub band and apply third level DWT to obtain LL3, HL3, LH3 and HH3.
Step8: Take the watermark image which is to be embedded in the host video frames and split it into red, blue and green components.
Step9: Convert the RGB components of the watermark image into grey component.
Step10: Apply wavelet transformation using db wavelets up to three level decomposition to obtain sub-bands LL3, HL3, LH3 and HH3.
Step11: The watermark bits are then embedded into significant coefficients of the host video frames.
Step12: Apply Inverse DWT to obtain the watermarked frames.
Step13: Reconstruct the watermarked video by combining frames.

Watermark Extraction Algorithm

The extraction procedure involves extracting the watermark from the host video in which it was embedded. Various steps are involved which are as mentioned below.

Step1: Read the watermarked video and split it into frames.
Step2: Convert the red, blue and green components into grey component.
Step3: Apply wavelet transformation using db wavelets up to three level decomposition to obtain sub-bands LL3, HL3, LH3 and HH3 for the watermarked frames.
Step4: Evaluate the difference between the LL3 frequency sub band of watermarked frame and the third level decomposed LL3 frequency sub band of the host frame to get the watermark.

5. CONCLUSION

Watermarks can be of the form images, text, binary logos, signatures, and numbers. They are used for storing information about the copyright owner, source of data, and authentic users. Watermarking technique plays useful role in many areas such as intellectual and copyright protection, authenticity check, fingerprinting applications, and can also be used in pan card details, employee id cards etc. The project work is based on two main viewpoints. The first viewpoint describes about the different watermarking techniques and showcases the comparative description of superiority of one technique over the other. It is seen that frequency domain is more suitable domain for watermarking schemes as it yields robust results as compared to other domains such as spatial domain. Also, it is concluded that discrete wavelet transform outperforms compared to discrete fourier and cosine transforms.

6. REFERENCES

[1]Yang Qianli, Cai Yanhong, "A Digital Image Watermarking Algorithm Based on Discrete Wavelet Transform and Discrete Cosine Transform", 978-1-4673-2108-2/12/$31.00 ©2012 IEEE

[2]Mehran Andalibi, Damon M. Chandler, "Digital Image Watermarking via Adaptive Logo Texturization", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 24, NO. 12, DECEMBER 2015

[3] Ghazy R A, El-Fishawy N A, Hadhoud M M, Dessouky M I and El-Samie F E A 2007 An efficient blockby-block

SVD-based image watermarking scheme. Radio Science Conference, NRSC 1–9

[4] Kasmani S A and Naghsh-Nilchi A 2008 A new robust digital image watermarking technique based on joint DWT-DCT transformation. Convergence and Hybrid Information Technology ICCIT '08 Third International Conference 2(1): 539–544

[5] Jianqin Zhou, Lingyun He, Cheng Shangguan "Watermarking Scheme Based on DCT and DHT" 2009 Second International Symposium on Electronic Commerce and Security 2009, Vol. 1,pp 223 – 227

[6]. Vidyasagar M. Potdar, Song Han, Elizabeth Chang"A Survey of Digital Image Watermarking Techniques", 3rd IEEE International Conference on Industrial Informatics (INDIN) 2005,pp-709-716.

[7]. Saba Riaz, M. Younus Javed, ,M. Almas Anjum "Invisible Watermarking Schemes in Spatial and Frequency Domains" IEEE International Conference on Emerging Technologies ,pp 211 – 216

[8] He, H. J., Zhang, J. S. and Tai, H. M., (2006), A Wavelet-BasedvFragile Watermarking Scheme for Secure Image Authentication. Springer-Verlag Berlin Heidelberg 2006

[9] Byun, S. C., Lee, S. K., Tewfik, A. H. and Ahn, B. H., (2003), A SVD-Based Fragile Watermarking Scheme for Image Authentication. Springer-Verlag Berlin Heidelberg 2003

[10] GAO Xin-yu, LV Jian-ping. A block-based DCT algorithm of Digital image watermarking., JOURNAL OF XI"AN UNIVERSITY OF POSTS AND TELECOMMUNICATIONS. Vol.12,No.5, sep.2007

[11] A. K. Soman, P. P. Vaidyanathan, and T. Q. Nguyen, "Linear phase paraunitary filter banks: Theory, factorizations and designs," IEEE Trans. Signal Process., vol. 41, no. 12, pp. 3480–3496, Dec. 1993.

[12] H. Zou and A. H. Tewfik, "Discrete orthogonal M-band wavelet decompositions," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, 1992, vol. 4, pp. 605–608

[13]Jeril George, Satishkumar Varma, Madhumita Chatterjee, "Color Image Watermarking using DWT-SVD and Arnold Transform", 2014 Annual IEEE India Conference (INDICON)

[14] Malihe Soleimani, Faezeh Sanaei Nezhad, Hadi Mahdipour and Morteza Khademi, "A Robust Digital Blind Image Watermarking Based on Spread Spectrum in DCT Domain," Science Academy Transactions on Computer and Communication Network, vol. 2, no. 2, pp. 122-126, June 2012.

[15] Mr.Navnath S. Narawade and Dr.Rajendra D.Kanphade, "DCT Based Robust Reversible Watermarking For Geometric Attack," International Journal of Emerging Trends & Technology in Computer Science, vol. 1, no. 2, pp. 27-32, August 2012.

[16] Mrs. Rekha Chaturvedi, Mr. Abhay Sharma, Mr. Naveen Hemrajani, Mr. Dinesh Goyal, "Analysis of Robust Watermarking Technique using Mid-band DCT domain for different image formats," International Journal of Scientific and Research Publications, vol. 2, no. 3, March 2012.

[17] Malihe Soleimani, Faezeh Sanaei Nezhad, Hadi Mahdipour and Morteza Khademi, "A Robust Digital Blind Image Watermarking Based on Spread Spectrum in DCT Domain," Science Academy Transactions on Computer and Communication Network, vol. 2, no. 2, pp. 122-126, June 2012.

[18] Mr.Navnath S. Narawade and Dr.Rajendra D.Kanphade, "DCT Based Robust Reversible Watermarking For Geometric Attack," International Journal of Emerging Trends & Technology in Computer Science, vol. 1, no. 2, pp. 27-32, August 2012.

[19] Mrs. Rekha Chaturvedi, Mr. Abhay Sharma, Mr. Naveen Hemrajani, Mr. Dinesh Goyal, "Analysis of Robust Watermarking Technique using Mid-band DCT domain for different image formats," International Journal of Scientific and Research Publications, vol. 2, no. 3, March 2012.

[20] Luigi Rosa, "High Capacity Wavelet Watermarking using CDMA Multilevel codes", Via Paolo della Cella 3, 10139, Turin, ITALY.

[21] Tarun Kumar and Karun Verma 2010" A Theory Based on Conversion of RGB images to Gray image " International Journal of Computer Applications (0975-8887) Volume 7- No.2 , September 2010