

Robust Image Watermarking in Frequency Domain

G. Dayalin Leena and S. Selva Dhayanithy

Department of Computer Science and Engineering,
Jerusalem College of Engineering, Anna University,
Chennai, Tamil Nadu, India

Copyright © 2013 ISSR Journals. This is an open access article distributed under the ***Creative Commons Attribution License***, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT: The spreading out of internet these days has raised the worth of digital media all over the planet. Digital watermarking has been a boon to digital media world as it endows various benefits like authentication, copy control and rights management of digital media. Digital images a category under digital media can be watermarked either in time domain or in frequency domain. The goal is to produce an efficient, secure and invisible watermarked image using digital watermarking thereby improving the quality and increasing the robustness of watermarked image. Here, digital image is watermarked using wavelet transforms which is an efficient multi-resolution frequency domain techniques. The low frequencies of wavelet decomposition of the carrier image which is a color image is watermarked with a color logo shuffled using a chaotic map technique. Embedding process is highly secured as chaotic map technique shuffles the watermark in order to confuse any unauthorized person who tries to modify or remove the corresponding watermark. The Peak Signal to Noise Ratio (PSNR) of watermarked image has proved that the original image and the watermarked image are visually indistinguishable by human observers. Robustness is checked well by extracting the original watermark perfectly without any degradation in the original image.

KEYWORDS: Arnold Cat Map, Discrete Wavelet Transform, Pixel Dependency, Robust, Watermarking.

1 INTRODUCTION

Years ago, it was almost unthinkable about how best to protect visual artists, photographers' images when distributed over the internet. The major challenge in finding copies of images on the web has always been a critical problem. Various approaches at different periods has been tried to address the above issue. But now we are in a very special age when it comes for the protection of digital images. The most effective approach for digital image protection is watermarking. watermarking is basically defined as any useful information embedded directly into the digital media itself by altering the image contents. Though most of all think image watermarking is the placing of a visual mark over an image, usually a logo a name, Watermarking here involves embedding an invisible watermark over an image that can only be detected by the owner of an image. The advantages of using digital watermark are numerous. They provide much more steadfast watermarks. Watermarks can, also survive great modification by users. Watermarked images can be detected perfectly after certain manipulations. Also, additional information about the owner of the image can be hidden in the image. an effective watermark should be robust to common image manipulations and unobtrusive so that it does not affect the visual quality of watermarked image. Digital watermarks have been broadly and successfully deployed in billions of digital images, across a wide range of applications. Some of applications include image security, image content identification and rights management. Image watermarking technique involves spatial and frequency domain as two different approaches. In spatial domain, luminance values of original image are altered in order to hide a watermark. Mostly, least significant bits original image are replaced with bits of watermark. But this approach falls down whenever there is a need to hide or large number of bits in an image. If large numbers of bits are modified in the original image, the pixel dependency will fail produce an efficient watermarked image. This issue has been dealt well by frequency domain techniques. The reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients. For example, the HVS is more sensitive to low-frequency coefficients, and less sensitive to high

frequency coefficients. In the case of one-dimensional signal, the signal is to be divided into two groups of frequency component as low frequency components and high frequency components which are mainly determined as the first pass the low-pass and high-pass frequencies. While the high-band frequency group would remain unchanged, the low-band frequency group is then divided into two other inner groups of frequencies causing the second pass of the low-pass and pass frequencies. The same process is to be continued in such an arbitrary number of times making the next passes by dividing the low-pass frequency blocks [1]. With regard to still images that consist of a two-dimensional signal, it is to be decomposed into DWT pyramid structure with various frequency bands. Discrete wavelet transform (DWT) is one of the powerful wavelet techniques of frequency domain which has a very low computational complexity. DWT decompose an image into various sub-bands in which the sub-bands provide separated low and high frequency wavelet coefficients. DWT has an utmost advantage of analyzing images of multi-resolution qualities. The wavelet transform is computed separately different segments of time-domain images at different frequencies. Multi-resolution analysis is designed to provide good quality time resolution and poor quality frequency resolution at high frequencies, and good quality frequency resolution poor quality time resolution at low frequencies. It's good for images having high frequency components for short and low frequency components for long durations. The wavelet function used to decompose an image is called Haar wavelet. This wavelet forms the basis of discrete wavelet transform. Haar wavelets are the oldest and simplest yet wavelet family. DWT has higher flexibility as wavelet functions can be chosen freely. Another technique which is a part in watermarking is chaotic map technique. Chaotic map is a vibrant scheme that relies greatly on its initial conditions which random and erratic. One of the remarkable individuality of chaotic map is if any one alters the initial conditions they will an entirely new outcome that will not be similar to the output of a different set with different initial conditions and that is why chaotic map are deterministic. A chaotic map known as the Arnold's Cat Map (ACM) is a discrete system that and folds up the trajectories in time space, which is a torus. ACM constantly apply its map to a given image and each of its iterations moves the image elements called pixels to a unique equivalent peak along the same torus. Ultimately the images will return to the original image at certain iteration.

2 RELATED WORKS

Analyses of various digital image watermarking techniques are explained in [2]-[4]. In [5] a new chaos based watermarking scheme for image authentication and tamper detection is introduced. This scheme provides both integrity authenticity for digital watermarking. Extracting the right watermark is only possible if someone has correct keys. Since chaotic maps are sensitive to initial values, they are used as key in this scheme. A person with wrong keys will not be able forge the watermark. In order to thwart counterfeiting attacks it is essential to break pixel wise independency, this employs chaotic maps to break the corresponding position relation between pixels in the watermarked image and the watermark. Provides high fidelity and is capable of localizing modified regions in watermarked image. [6] Proposed an watermarking technique based on Singular Value Decomposition and Tiny-Genetic Algorithm. The singular values of the cover image are modified to embed the watermark. The Tiny-GA offers a systematic way to consider the improvements of the scaling factors that are used to control the strength of the embedded watermark. With this scheme, embedded watermark successfully survived after attacked by image-processing operations. Simulation results show that the scheme outperforms the other similar works. [7] Proposed a novel asymmetric watermarking scheme. Both the user side watermark and copyright owner's one are generated from the copyright owner's private keys, and the watermark can be finished either by public watermark or the copyright owner's private one. Given the public watermark, it is to guess or remove the embedded watermark. Experimental results against removal attack and Jpeg compression show robustness in this scheme. [8] Proposed a novel digital watermarking scheme for color image, watermarking image was embedded into the corresponding wavelet coefficients of the original image's R, G, B sub images via discrete wavelet transform. The availability of the extracted watermark is evaluated by comparing the normalized correlation coefficients the extracted watermark with the original one. Experiment results show high robustness of this approach to the common image processing technique such as JPEG compression and additive noise etc. [9] Development of new multimedia services and environments requires new concepts both to support the new working process and to protect the multimedia data during the production and distribution. This scheme addresses image video authentication and copyright protection as security demands in digital marketplaces. First a content-based signature technique for image and video authenticity and integrity is presented. Based on this technique, a tool for interactive video authentication and propose content fragile watermarking, a concept which combines watermarking and content-based digital signatures to ensure copyright and detection of integrity violation have been implemented. DWT based watermarking algorithm of color images is in [10]. This method dealt with JPEG Compression attack and achieved good result. Watermarking using multi-resolution wavelet decomposition is proposed in [11]. He decomposed the cover image into non overlapping multi-resolution wavelet decomposition and used the decomposed level for watermarking. His scheme proved increased robustness of watermarked images and resist to most image processing attacks. A robust logo image watermarking is proposed in [12].

used a binary logo as the watermark image. Independent Component Analysis is done for the images and then embedded with the logo watermark which proved high imperceptibility of watermarked images.

3 PROPOSED WORK

The proposed system effectively and securely embeds a color carrier image with a color watermark. Carrier image of any size is taken for the experiment. Carrier image taken as input is employed with single level DWT decomposition. The decomposition of DWT includes four different sub-band levels low-low (ll), low-high (lh), high-low (hl) and high-high (hh) respectively. The low-low sub-band of first level is then decomposed to get the second decomposition level. The low-low sub-band of second level is further decomposed till the fifth level of Discrete Wavelet Transform decomposition is obtained. Watermark taken is resized according to the last decomposed size of carrier image. The resized watermark is then employed with Arnold's Cat Map transforms a chaotic map technique. The last low-low sub-band of carrier image is embed with the Arnold shuffled watermark using embedding principle. Apply inverse DWT on the embedded coefficients to get the watermarked image. Fig. 1 shows the embedding architecture diagram.

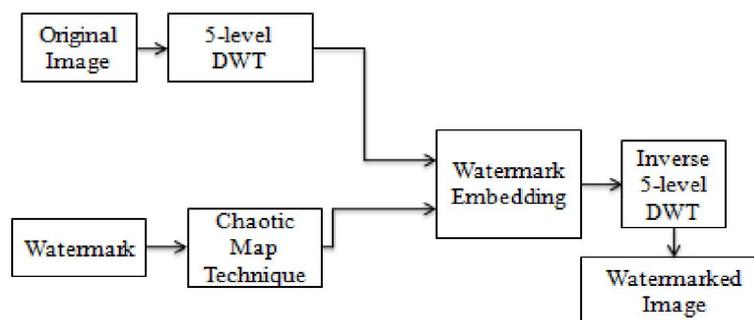


Fig. 1. Embedding Architecture

3.1 TRANSFORM MODULE

Carrier image is separated into R, G, B component where each of separated component forms gray images. The watermark taken is resized by removing the unwanted pixels if any. Resizing is purely depending on the final decomposed level of carrier image. For example, if the carrier image taken is of size 512*512 and the last decomposed level is of size 16*16 then the watermark taken should be resized to 16*16 whatever the actual size may be. There are two transforms applied in this form of watermarking, one for original image and one for watermark. Transform module is the important part in watermarking a digital image as it provides the frequency components on which the watermark is done. Discrete Wavelet Transform (DWT) is the transform applied on the original watermark. DWT decomposes the original image into different wavelet coefficients, one fine grained frequency level and three coarse grained frequencies. The fine grained frequency is perceived more by the human vision whereas the coarse grained frequencies are less perceived by the human vision (HVS). Mostly watermarking is done in high frequencies which are less perceived. The four different levels are named as oll (approximation), olh (horizontal), ovl (vertical), and ovl (diagonal) levels respectively. To get the second level of decomposition, the approximation sub-band of first decomposition level is taken and decomposed further, likewise for all the five decomposition levels. The decomposition is done using a simplest and basic transformation from the space/time domain into a local frequency domain namely Haar transform. The Haar transform serves as a prototype for the wavelet transform, and is closely related to the discrete wavelet transform. The Haar transform uses Haar function for its basis. The Haar function is an ortho normal, rectangular pair. Compared to the Fourier transform basis function which only differs in frequency, the Haar function varies in both scale and position. It has some desirable properties such as supporting continuous and discrete transforms, fast algorithm and exact reconstruction of images. Arnold's Cat Map Transform (ACM) is applied on the watermark to shuffle the watermark. The exact illustration of chaos we look at here is the chaotic mapping called Arnold's cat map as a gratitude of a Russian mathematician Vladimir I. Arnold, who revealed it by means of an image of a cat. ACM is an easy and refined manifestation and illustration of a principle of chaos namely, fundamental categorization to an actually an indiscriminate growth of a system. Any image that is hit with a transformation in fact randomizes the unique union of its elements. On the other hand, if iterated adequate times, magically, the original image recurs.

3.2 WATERMARKING MODULE

This module includes watermark embedding and watermark extraction. Watermark embedding is a process of inserting a watermark into a host/original image. A watermark is placed into information content of original image to create watermarked image. A simple diagrammatic representation of embedding is given in Fig. 2, where $I(x, y)$ is the original image, $W(x, y)$ is the watermark and $I_w(x, y)$ is the watermarked image. The invisibility of embedding is based on the weight added. The weight of watermark is taken as the scaling factor for both embedding and extraction process.

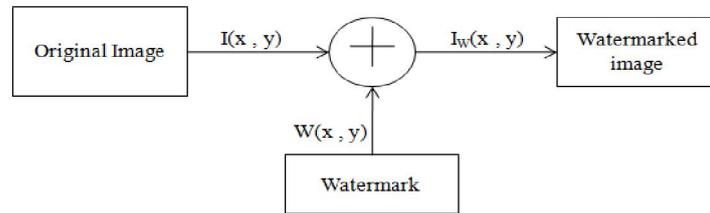


Fig. 2. Basic Embedding Principle

4 WATERMARKING PROCESS

4.1 WORKFLOW DIAGRAM

The process flow diagram showing the detailed levels of channel separation of cover image, Arnold scrambling of watermark image and embedding algorithm are shown in Fig. 3. After embedding the fifth approximation level of each component with the scrambled watermark, inverse DWT is applied on the each embed component. All the three components are merged together to form the watermarked image.

4.2 WATERMARKING ALGORITHM

Step 1: Color image of size 512*512 is taken as the input. Images of different sizes and formats can also be taken as original images as they are used and verified for embedding.

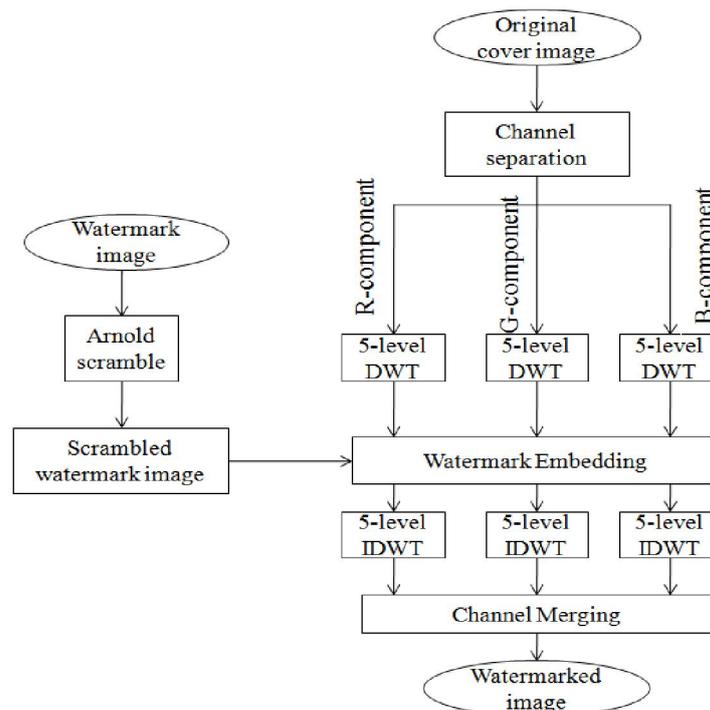


Fig. 3. Embedding Workflow

Step 2: Separate red, green and blue components from the original image.

Step 3: Name the component as $fr(i, j)$, $fg(i, j)$ and $fb(i, j)$, where $fr(i, j)$ is the separated red component image; $fg(i, j)$ is the separated green component image and $fr(i, j)$ is the separated blue component image.

Step 4: Decompose each separated component of original image using discrete wavelet transform into five level wavelet coefficients. The fifth level wavelet decomposition principle is given in Eq. (1)

$$Y(2n+1) = X(2n+1) - [(X(2n) + (2n+2))/2]$$

$$Y(2n-1) = X(2n-1) + [(Y(2n-1) - Y(2n-2))/5] \quad (1)$$

Step 5: Take the fifth level low frequency wavelet coefficient. After fifth level decomposition the size of image is reduced from 512×512 to 16×16 . Let the coefficients be $ll5$, $lh5$, $hl5$ and $hh5$. $ll5$ is taken for watermark embedding.

Step 6: Read color watermark of any size as it is resized to the size of $ll5$ before watermarking. Watermark of size 256×256 is taken for initial experiment.

Step 7: Rescale the watermark to size 16×16 using bilinear interpolation method.

Step 8: Apply Arnold's cat map transform on the rescaled watermark in which the watermark now becomes a chaos of pixels instead of a proper image.

Step 9: Now embed shuffled watermark with the $ll5$ decomposed level of original image. The embedding principle is given in Eq. (2) where W_{mi} is the watermarked image; 'f' is the scaling factor; $ll5$ is the approximation sub-band of fifth level decomposition; Wm is the Arnold shuffled watermark.

$$W_{mi} = (ll5 + f * Wm) \quad (2)$$

Step 10: Embedding technique is applied for the entire three separated component.

Step 11: Apply inverse 5-level discrete wavelet transform (IDWT) on each of the embedded image coefficients.

Step 12: Merge the three embedded image coefficients to produce the watermarked image.

Step 13: The extraction process follows the principle as in Eq. (3)

$$WM = (W_{mi5} - ll5) / f \quad (3)$$

Step 14: WM is the watermark to be extracted, W_{mi5} is the fifth decomposed level of watermarked image; 'f' is the scaling factor; $ll5$ is the fifth decomposed level of original image.

5 IMPLEMENTATION RESULTS

Input image of dimension 512×512 , watermark of size 256×256 are taken for embedding process. Watermark is resized based on the level of decomposition of input image. Image taken for watermarking are, a color fairy image as the carrier image and a color logo as the watermark. Fig. 4 shows the diagrammatic representation of result which includes the original image, the watermark, watermarked image and the extracted watermark.

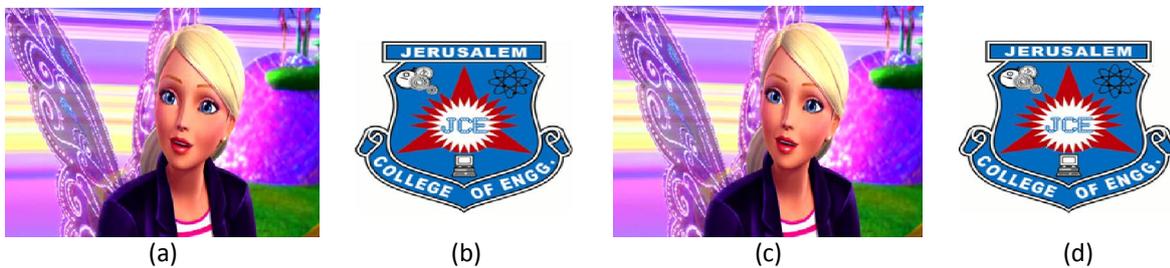


Fig. 4. (a) Original Image (b) Watermark (c) Watermarked Image (d) Extracted Watermark

Mean Square Errors and Peak Signal to Noise Ratios are calculated for watermarked images calculated using (3) for watermarked image and found to be relatively high.

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right)$$

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N} \quad (3)$$

Where, 'R' is the highest variation in the input image data type. For example, if the input image has a double-precision floating-point data type, then the value of R is 1. If it has an 8-bit unsigned integer data type, the value of R is 255. M and N are the number of rows and columns in the input images. $I_1(m, n)$ is the original image and $I_2(m, n)$ is the watermarked image. Table 1 shows the PSNR for watermarked images with different scaling factors. PSNR rate for watermarked image is compared from level-1 to level-5 and the fifth level watermarked image reached 48.0547. This proved the level of watermarking has been increased considerably.

Table 1. Comparison of Level-1 to Level-5 Dwt for Watermarked Image in Terms of PSNR

f	PSNR Level 1	PSNR Level 2	PSNR Level 3	PSNR Level 4	PSNR Level 5	Observation
0.005	28.4505	29.6219	29.683	31.1111	31.2814	
0.002	30.6518	30.7788	31.1263	32.7223	32.777	
0.02	42.440	43.640	45.897	46.9358	48.0547	Best Result
0.10	42.006	42.121	42.8262	43.078	45.3502	
0.15	37.1331	37.2139	37.9877	38.0001	38.396	

6 CONCLUSION

An efficient digital watermark scheme must meet three main properties: security, imperceptibility and robustness. All the above properties are met by this method of watermarking. Images are securely watermarked so that no unauthorized person can detect or remove watermark from the watermarked image. In future, image robustness can be checked well by including attacks and extracting the watermark from the attacked watermarked image without any quality degradation in the original image.

REFERENCES

- [1] Heena Shaikh, Mohd. Imran Khan, and Yashovardhan Kelkar, "A Robust DWT Digital Image Watermarking Technique Basis on Scalling Factor," *Int. J. Computer Science, Engineering and Applications*, vol. 2, n^o. 4, Aug. 2012.
- [2] Keshav S Rawat and Dheerendra S Tomar, "Digital Watermarking Schemes for Authorization against Copying or Piracy of Color Images," *Indian Journal of Computer Science and Engineering*, vol. 1, n^o. 4, pp. 295-300.
- [3] Manpreet Kaur, Sonika Jindal, and Sunny Behal, "A Study of Digital Image Watermarking," *International Journal of Research in Engineering & Applied Sciences*, vol. 2, Issue 2, pp. 226-236, 2012.
- [4] Mansi Hasija and Alka Jindal, "Contrast of Watermarking Techniques in different domains," *IJCSI International Journal of Computer Science Issues*, vol. 8, Issue 3, no. 2, pp. 559-563, May 2011.
- [5] Sanjay Rawat and Balasubramanian Raman, "A chaotic system based fragile watermarking scheme for image tamper detection," *Int. J. Electron. Commun*, vol. 65, pp. 840-847, Jan. 2011.
- [6] Chih-Chin Lai, "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm," *Int. Con. Digi Sig Processing*, vol. 21, pp. 522-527, 2011.
- [7] Yong-Gang Fu, "Asymmetric Watermarking Scheme Based on Shuffling," *Int. WIEE*, vol. 29, pp. 1640-1644, 2012.
- [8] Zhou Zude, Ai Qingsong, and Liu Quan, "Digital Watermarking Scheme for Color Image Based on Image Fusion," *Proc. ICWMM*, 2006.
- [9] J. Dittmann, A. Steinmetz, and R. Steinmetz, "Content-based digital signature for motion pictures authentication and content-fragile watermarking," in *Proc. IEEE Int. Conf. Multimedia Computing System*, pp. 209-213, 1999.
- [10] Baisa L. Gunjal and Suresh N.Mali, "Secured color image watermarking technique in DWT - DCT domain," in *Proc. Int. J. Computer Science, Engineering and Information Technology (IJCEIT)*, vol. 3, Issue 1, 2011.
- [11] Ghouti L, Bouridane A and Ibrahim MK, "Digital image watermarking using balanced multi-wavelets," *IEEE Transactions on Signal Processing*, vol. 54, Issue 4, pp. 1519-1536, 2006.
- [12] Amol R. Madane, K T. Talele and M. M. Shah, "Watermark Logo in Digital Image using DWT", in *proceedings of International Conference on SPIT*, Mumbai, India, vol. 1, 2008.