International J. of Math. Sci. & Engg. Appls. (IJMSEA)
ISSN 0973-9424, Vol. 10 No. III (December, 2016), pp. 77-89

A DUAL WATERMARKING USING DWT, DCT, SVED AND IMAGE FUSION

NARENDRAKUMAR R. DASRE
Department of Engineering Sciences,
Ramrao Adik Institute of Technology, Nerul,
Navi Mumbai-400706, India

Abstract

This paper presents blind and non blind digital image watermarking algorithm based on two dimensional discrete wavelet transform. In this paper, two watermarks are embedded in two different wavelet channels. First watermark is embedded using non-blind technique which is based on singular value decomposition and discrete cosine transform. Second watermark is embedded using blind technique based on image fusion. The proposed algorithm is secured because instead of inserting watermark as it is in a wavelet channel, watermark is encrypted using cat mapping and then inserted into the desired wavelet channel. Also there are many parameters that can be used as a security key like the iterative time of the Arnold transform, wavelet channel, scaling factor etc. It is also possible to change initially selected parameters. After reconstruction, watermark image is extracted by applying inverse cat mapping. Algorithm was tested using different powerful attacks like bit compression, JPEG compression, median filtering, image cropping, rotation etc. Experimental results found support the robustness and security of the proposed algorithm.

Key Words : *DCT, SVD, Image fusion, Cat mapping, Blind watermarking, Normalized correlation coefficient, PSNR.*

1. Introduction

With the growth of the Internet and immediate availability of computing resources to every individual, digital content can be reproduced and distributed immediately with no effort and at no cost. Hence to protect and preserve the digital intellectual property and to encourage the creators of digital content, it has become very necessary to develop some means or methods. Hence digital watermarking which can be applied to image, audio, video, text and data is developing at a fast rate since the last twelve years.

Though there are various other applications, copyright protection and image authentication are the two main applications of digital image watermarking. More and more algorithms are being developed every day based on the invention of different transforms. Each new developed algorithm seems to be able to withstand various attacks like jpeg compression, median filtering, image cropping, rotation, scaling, bit compression etc. But the universal algorithm that can withstand all possible attacks and image processing operations is still not developed because it is difficult to visualize what ideas may emerge in a hacker's mind to attack the digital content. This is the reason why the field of digital watermarking is relatively new and has the potential for tremendous growth. Watermarking algorithm must be able to satisfy all these requirements.

1. Imperceptibility: The data embedding process should neither introduce any perceptible or noticeable artifact into the host image nor degrade the perceived quality of the host image.

2. Robustness: The watermark should still be present in the image after a possible distorted attack and should be detected by the watermark detecting algorithm, especially to the attack from jpeg compression or median filtering or other image processing operations.

3. Unambiguousness: A watermark should convey as much information as possible. A watermark should statistically be undetectable. Moreover, the extracted watermark can be used to identify the ownership and copyright unambiguously.

4. Security: A watermark should only be accessible the authorized parties. As the information security technique, details of the digital watermarking algorithms must be published to everyone and only the owner of digital content must hold the

private keys. Watermarking techniques mainly falls in two categories- a) Spatial domain method [1,2] and b) spectral domain method [3, 4].

a) Spatial domain method: In this, watermark is embedded directly by modifying the pixel location of the images. These methods are less complex as no transform is used but are not robust even against simple attacks. Also they have relatively low bit embedding capacity and are not resistant enough to lossy image compression. The simplest example based on these methods is to embed the watermark in the Least Significant Bits (LSB) of image pixels [5].

b) Spectral domain method: In these methods, the image is transformed into a set of a frequency domain coefficient using discrete cosine transform(DCT), discrete Fourier transform (DFT) or the discrete wavelet transform(DWT). Watermark is then inserted into an image by modifying selected frequency coefficients of image pixels. These methods can embed more bits of watermark and are more robust to attacks. But both the techniques discussed above have the same defect that they modify working pixels of original image.

2. Preliminary

In this section, we have discussed the preliminary requirements.

A. DWT of the image:

The wavelet transform is identical to a hierarchical subband system, where the subbands are logarithmically spaced in frequency. The basic idea of the DWT for a two dimensional image is described as follows. An image is first decomposed into four parts of high, middle and low frequencies (i.e. LL_1, HL_1, LH_1, HH_1 subbands) by critically subsampling horizontal and vertical channels using Daubechies filters [6]. The sub band HL_1, LH_1 and HH_1 represent the finest scale wavelet coefficients. To obtain the next coarser scaled wavelet coefficient, the subband LL_1 is further decomposed and critically subsampled. This process is repeated several times, which is determined by the application in hand. An example of an image decomposed into seven subbands for two levels is shown in Figure 1. Each level has various bands information such as low-low, low-high, high-low and high-high frequency bands.

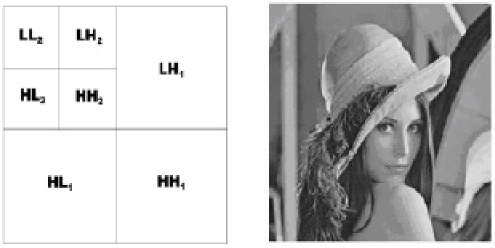


Figure 1: Decomposition and Lena Image.

Furthermore, from these DWT coefficients, the original image can be reconstructed. For reconstruction process same filter must be used. This reconstruction process is called the inverse DWT (IDWT). If I (m, n) represent an image, the DWT and IDWT for I (m, n) can be similarly defined by implementing the DWT and IDWT on each dimension m and n separately [7].

B. Arnold Transform:

Arnold transform is also called Cat mapping[13, 14]. It is used to scramble the digital image. The digital image is nothing but a matrix of pixels. Each pixel has a unique position in terms of image height and width and has different gray level value. For a digital image with size $N \times N$, cat mapping of pixel co-ordinate (x, y) is

$$\begin{bmatrix} x\prime \\ y\prime \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} modN$$

where x, y $\epsilon 0, 1, \cdots, 2N-1$. Here mod N represents modulo operation and $(x\prime, y\prime)$ represents new position of pixel after scrambling by Arnold transform[13]. In order to ensure that cat mapping is one to one mapping, the value of the matrix A should meet the requirement of $|A| = 1$. So the matrix A can be simply given by

$$A = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix}$$

where a and b both are integers. The basic principle of cat mapping is to arrange the location of pixels within the image. It achieves its objectives of encryption by disturbing the position of pixels [8, 9]. The iterative formula of cat mapping can be expressed as-

$$P_{x,y}^{n+1} = AP_{x,y}^{n} modN$$

Where in above equation $P^n_{x,y} = (x,y)^T$ and n = 0, 1, 2, . . .is the times iterative transformation and A is matrix of Arnold transform. Because of the limit of $N \times N$ pixel performance, the process has iteration period. The period of the iteration [10, 13, 14] for various size N of an image is given as in table I.

Relation between Image size (N) and Iteration period of Arnold Transform

N	2	4	5	8	10	16	32	64	128	256
Period	3	3	10	6	30	12	24	48	96	192

Once cat mapping is applied to the original watermark image W_0, it is easy to get W_0 back by taking inverse Arnold transform until iteration period.

C. Singular Value Decomposition:

If an m x n image is represented as a real matrix A, it can be decomposed as:

$$A = USV^T$$

It is called a singular value decomposition of A. Where U is an m x m unitary matrix, S is an m x n diagonal singular matrix with nonnegative numbers on the diagonal and zeros on the off diagonal and V^T denotes the conjugate transpose of V where V is n x n unitary matrix. Note that U and V are orthogonal or unitary. Use of SVD in digital image processing has some advantages. First, the size of the matrices from SVD transformation is not fixed. Secondly, singular values in a digital image are less affected if general image processing is per No. of bits used to represent the original image formed. Finally, singular values contain intrinsic algebraic image properties.

D. Discrete Cosine Transform:

The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies. The DCT has the property that, for a typical image, most of the visually significant information about the image is concentrated in just a few coefficients of the DCT. For this reason, the DCT is often used in image compression applications. The constant-valued basis function at the upper left is often called the DC basis function, and the corresponding DCT coefficient is often called the DC coefficient. DCT uses only cosine waves to represent two dimensional signals as given below.

$$F(u,v) = A\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right]$$

Where $A = \alpha(u)\alpha(v)$, for $u, v = 0, 1, 2....N-1$ and

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} AF(u,v)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right]$$

for x, y = 0, 1, 2...., N-1.

E. Invisibility Testing of the Watermarked Image:

The inserted watermark(logo) into an image I_0 should not provide any visible artifacts noticeable to human eye i.e. I_0 and I_w must be exactly same. The extent up to which this is achieved is expressed by peak signal to noise ratio (PSNR). PSNR of image of size $N \times N$ is given by equation

$$PSNR = 10log_{10}\left[\frac{N \times N \times max(I_w)^2}{\sum_{i=0}^{N}\sum_{j=0}^{N}(I_0 - I_w)^2}\right]$$

where $I_0(i,j) = I_0$ and $I_w(i,j) = I_w$.

F. The Robustness Testing of the Watermarked Image:

The original watermark (W) and extracted watermark ($W\prime$) must be exactly same. The extent up to which this is achieved is expressed by normalized correlation coefficient (NC). Its value equal to unity indicates that W and $W\prime$ are exactly same. Thus $NC = 1$ indicates perfect robustness of the algorithm. NC for watermark image W of size $M \times M$ is given by following equation

$$NC = \frac{\sum_{i=0}^{M}\sum_{j=0}^{M} W(i,j) \times W\prime(i,j)}{\sum_{i=0}^{M}\sum_{j=0}^{M} W(i,j) \times W(i,j)}$$

3. Proposed Algorithm

In this section, we consider the watermark embeding and exttraction processes. First we consider the watermark embedding process. Then we consider tghe extraction process.

A. Watermark Embedding Algorithm:

To embed the watermarks, we use the following steps [11, 12, 14].

1. Let I_O be an original image of size 512×512. Perform two level decomposition of the original image to get seven sub-bands LL_2, HL_2, LH_2, HH_2, HL_1, LH_1 and HH_1.

2. Divide LL_2 band into a 1024 square blocks of 4×4 dimension each, apply discrete cosine transform to each block and collect total 1024 DC value from these blocks. These DC values will form new matrix D of size 32×32.

3. Apply single value decomposition (SVD) to D, i.e. $D = U_1 * S_1 * V_1^T$ and obtain U_1, S_1 and V_1.

4. Let W_1 be the first watermark image of size 32×32. Apply cat mapping to W_1 to get cat mapped watermark WC_1. Then modify S_1 with WC_1 i.e. perform $S_1 + \alpha * WC_1$ where α is scaling factor and apply SVD to it i.e.$S_1 + \alpha * WC_1 = U_2 S_2 V_2^T$ and obtain U_2, S_2 and V_2.

5. Obtain D^* by inserting S_2 in $D = U_1 S_1 V_1^T$ i.e. $D^* = U_1 S_2 V_1^T$.

6. Return all 1024 elements (DC coefficients) of D^* to 1024 blocks of LL_2. Apply inverse DCT to all 1024 blocks to produce the watermarked low frequency band LL_2^*.

7. Let W_2 be the second watermark image of size 32×32. Apply cat mapping to W_2 to get cat mapped watermark WC_2.

8. Embed cat mapped watermark WC_2 in any wavelet channel C of original image I_O except LL_2 by following equation [12].

$$C(n,m) = \begin{cases} C(n,m) & \text{if } 0 \leq n < \frac{N}{8} - M \\ & \text{and } 0 \leq m < \frac{N}{8} - M \\ k * M\big(n - \frac{N}{8} + M, m - \frac{N}{8} + M\big) & \text{otherwise} \end{cases}$$

   where $0 \leq n \leq \frac{N}{8}$ and $0 \leq m \leq \frac{N}{8}$ and k is scaling factor similar to α. Both scaling factors will take positive values.

9. Apply inverse discrete wavelet transform to $LL_2^*, HL_2, LH_2, HH_2, HL_1, LH_1, HH_1$ to get watermarked image I_W. This is a reconstructed image. Note that, theoretically $I_O = I_W$.

B. Watermark Extraction Algorithm:

To extract the embedded watermarks, we use the following steps.

1. Perform two level decomposition of the watermarked image I_W to get seven sub-bands $LL_2^*, HL_2, LH_2, HH_2, HL_1, LH_1$ and HH_1.
2. Divide LL_2^* band into 1024 square blocks of 4 $times4$ dimension each, apply DCT to each block. Collect the 1024 DC value from each block to get new matrix D^{**} of size 32×32.
3. Apply SVD to D^{**} i.e. $D^{**} = U_3 S_3 V_3^T$ and obtain S_3.
4. Obtain $E = U_2 S_3 V_2^T$ and also obtain the extracted watermark $WC_1\prime = (E - S - 1)/\alpha$.
5. Apply inverse cat mapping to the extracted watermark $WC_1\prime$ to get first extracted watermark $W_1\prime$. Note that $W_1 = W_1\prime$ theoretically.
6. Measure normalized correlation coefficient (NC) between the embedded watermark W_1 and the extracted watermark $W_1\prime$.
7. Extract cat mapped watermark $WC_2\prime$ from the watermarked image IW by the following equation [12]

   $$W\prime = k^{-1} * C\big(n + \tfrac{N}{8} - M, m + \tfrac{N}{8} - M\big)$$

   where $0 \le n \le \frac{N}{8}$ and $0 \le m \le \frac{N}{8}$ and k is scaling factor.
8. Apply inverse cat mapping to the extracted watermark $WC_2\prime$ to get the second extracted watermark $W_2\prime$. Note that $W_2 = W_2\prime$ theoretically.
9. Measure the normalized correlation coefficient (NC) between the embedded watermark W_2 and extracted watermark $W_2\prime$.

4. Experimental Results

We tested the proposed algorithm using 512×512 Lenagray level image. The first watermark (W_1) is RAIT NERUL of the size 32×32. This watermark is encrypted using cat mapping and inserted into LL_2 band using DWT, DCT and SVD. The second watermark (W_2) is alphabet D of the size 32×32. This watermark is also encrypted using cat mapping and inserted into one of the HH_2 or HL_2 or LH_2 band using image fusion technique. The watermarked image is reconstructed by IDWT. Then both watermarks are extracted from a watermarked image using inverse cat mapping. Figure 2 shows original image I_0, watermarked image I_W, embedded watermarks W_1 and W_2, extracted watermarks $W_1\prime$ and $W_2\prime$ for the embedding and extraction process.

Figure 2: Original Image, Watermarked Image, Original and Extracted Watermarks

From Figure 3 to 8 show watermarked image I_W and the extracted watermark $W_1\prime$ and $W_2\prime$ after bit compression attack, image cropping attack, Jpeg compression attack, median filtering attack, rotation attack and salt and pepper noise attack.

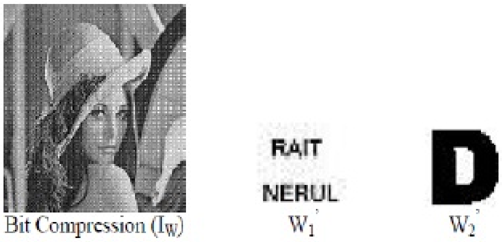


Figure 3: Bit Compression Attack

Cropping (25%) (I_W) W_1' W_2'

Figure 4: Image Cropping Attack

Jpeg (10%) attack (I_W) W_1' W_2'

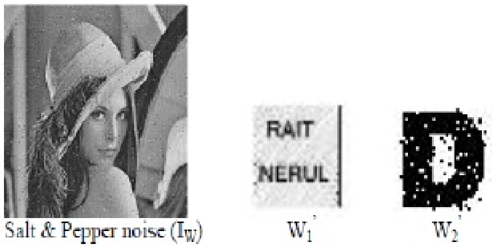
Figure 5: Jpeg Compression Attack

Median filtering (I_W) W_1' W_2'

Figure 6: Median Filtering Attack

Rotation (5deg) (I_W) W_1' W_2

Figure 7: Rotation Attack



Salt & Pepper noise (I_W) W_1' W_2'

Figure 8: Salt and Pepper Noise Attack

Table 2 shows statistical data for different attacks and different values of scaling factor k.

Statistical data for different attacks

Attack	K	RImage	R1logo	R2logo	SNR (dB)	PSNR (dB)
Bit Compression	0.01	0.7451	1	0.9917	9.036	19.17
	1	0.7605	1	1	8.8664	19.087
	5	0.7797	1	0.9363	5.3489	17.18
Image Cropping	0.01	0.0282	0.2763	0.9917	0.7706	6.802
	1	0.0154	0.4807	1	0.7507	7.1715
	5	0.0489	0.5118	0.9363	0.6624	8.1879
JPEG Compression	0.01	0.998	0.8391	0.7443	32.371	38.4019
	1	0.9851	0.9975	0.5033	22.555	28.9758
	5	0.8624	0.9549	0.9184	7.7587	17.8701
Median Filtering	0.01	0.998	0.88	0.1198	32.371	38.4019
	1	0.9851	0.9975	0.5033	22.555	28.9758
	5	0.8624	0.997	0.4382	7.7587	17.8701
Rotation	0.01	0.998	0.8363	0.0675	32.371	38.4019
	1	0.9851	0.916	0.0231	22.555	28.9758
	5	0.8624	0.9409	0.0228	7.7887	17.8973
Salt and Pepper	0.01	0.998	0.7919	0.1152	32.371	38.4019
	1	0.9851	0.8142	0.9709	22.555	28.9758
	5	0.8624	0.0282	0.0129	7.7587	17.8701

Graphs are plotted for NC of original image and watremarked image (RImage), NC of first original and extracted watremark (R1logo), NC of second original and extracted watremark (R2logo), SNR (dB), PSNR (dB) as a function of scaling factor k. RImage indicates the degree of similarity between original image I_0 and watermarked image I_W. Its value must be close to unity. If RImage=1, this means that original image I_0

and watermarked image I_W are exactly same. R1logo and R2logo represent normalized correlation coefficient i.e. NC_1 and NC_2 respectively. Their values must be close to unity. If $NC_1 = NC_2 = 1$, this means that the embedded watermark and extracted watermark are exactly the same. Figure 9 and Figure 10 shows graphs for NC and SNR, PSNR verses scaling factor.

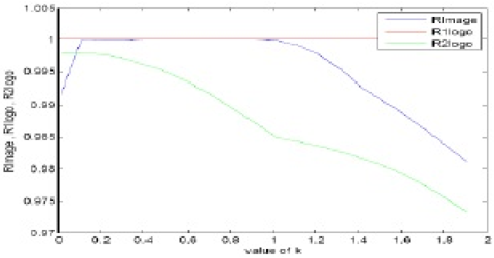


Figure 9: Graph for NC verses scaling factor k

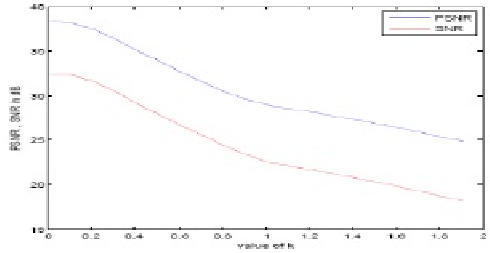


Figure 10: Salt and Pepper Noise Attack

5. Conclusion

From the results obtained in the form of images and graphs, it can be concluded that any attack cannot eliminate both the watermark simultaneously. The performance of the algorithm is very good for bit compression, cropping and salt and pepper noise attack. The performance of the algorithm is also good for median filtering attack. The performance of the algorithm is average for jpeg compression and rotation attack.

Acknowledgements

I am grateful to Dr. Ramesh Vasappanavara, Principal, RAIT, Nerul for his continuous support and guidance throughout the work.

References

[1] Bors A. G. and Pitas I., Image watermarking using DCT domain constraints, Proc. of IEEE Int. conf. on Image Processing, 3 (1996), 231-234.

[2] Van Schyndel R. G., Tirkel A. Z. and Osborne C. F., A digital watermark, Proc. of Int. conf. on Image processing, 2 (1994), 86-90.

[3] Ohnishi J. and Motsui K., Embedding a seal into a picture under orthogonal wavelet transformation, proc. of Int. conf. on multimedia comp. and system, (1996-6), 514-521.

[4] Kundur D. and Hatzinakos D., A robust digital image watermarking method using wavelet based fusion, Proc. of IEEE Int. conf. on Acoustic, speech and signal processing, 5 (1997), 544-547.

[5] Wolfgang R. and Delp E., A watermark for digital Image, Proc. Int .conf. Image processing, 3 (1996), 211-214.

[6] Wang Y., Doherty J. F. and Van Dyck R. E., A wavelet-based watermarking algorithm for ownership verification of digital images, IEEE trans.on Image Processing, 11(2) (2002), 77-88.

[7] Wen X. C. and Jing C., An anti-stastitical analysis LSB stegnography, incorporating extended cat mapping, Berlin Heidelberg, 12(5) (2007), 468-476.

[8] Franqois G., Diffusion, approximation and Arnold cat map, IEEE Transaction on image processing, 5(4) (1996), 179-190.

[9] Xie J., Xie Q. and Da-zu H., The periodicity and security analysis of Arnold transform, Network and Computer security, 5 (2008), 6-8.

[10] Wang B., Ding J. and Liao X., An image watermarking algorithm based on DWT, DCT and SVD, IEEE Proceeding of IC-NIDC, (2009), 1034-1038.

[11] Dasre N. R. and Patil H. R., On watermarking in frequency domain, 2^{nd} ICDIP, Proc. of SPIEx, 7546 (2010), 754622-1-5.

[12] Dasre N. R. and Patil H. R., A technique of watermarking using wavelet, Proceedings of IC-RAMSA, (2011), 420-427.

[13] Dasre N. R., On Watermarking Using Arnold and Wavelet Transform, IJMCR, 4(5) (2016), 1325-1332.

[14] Dahake V. R., Dasre N. R. and Gaikwad V. B., Digital Image Watermarking In Frequency Domain Using CAT Mapping, JSTM, 4 (2011), 11-16.