Techniques used for Digital Watermarking

Prof.P.T.Suradkar, Ashwini Kamble, Chaitrali Bhagat, Sneha Kadam,

ME, Computer Engineering, NBNSSOE, Maharashtra, India
BE, Computer Engineering, NBNSSOE, Maharashtra, India
BE, Computer Engineering, NBNSSOE, Maharashtra, India
BE, Computer Engineering, NBNSSOE, Maharashtra, India

ABSTRACT

Hybrid Image watermarking scheme proposed based on Discrete Cosine Transform (DCT)-Discrete Wavelet Transform (DWT)-Singular Value Decomposition (SVD). The cover image is reordered before DCT is applied. The DCT coefficients of the reordered image are decomposed into sub bands using DWT. The singular values of the middle sub bands are found and watermark is embedded. Simulation results shows that this method can survive attacks like rotation, cropping, JPEG compression and noising attacks and also can be used for copyright protection of multimedia objects.

Keyword :- *Discrete Wavelet transforms , Singular Value Decomposition, Discrete cosine transform.*

1. INTRODUCTION

Digital Watermarking is a technique to embed an imperceptible data called "watermark" into multimedia objects so as to discourage unauthorized copying or attesting the origin of the images. The invisible watermark is embedded in such a way that the modification made to the pixel value is perceptually not noticed, and it can be recovered only with an appropriate extraction mechanism. The embedding of the watermark into the cover image must be done in such a way to achieve efficient tradeoffs among the three conflicting objectives of maximizing the strength of watermark to be inserted, minimizing distortion between the cover image and watermarked image, and maximizing the resilience to attacks. The effectiveness of a digital watermarking algorithm is indicated by the robustness of watermarked signal against degradations. These degradations may result from processing and transmission or from deliberate/intentional attacks. Deliberate attacks are performed to destroy the watermark.

Watermarking can be categorized according to their processing domain, signal type of the watermark, and hiding location. Watermark embedding is performed in either spatial domain or frequency domain. There are different types of attacks: geometrical attacks, noising attack, de-noising attack, compression attack and image processing attack. Geometrical attack causes synchronization errors during the extraction process of the watermark due to which the quality of the extracted watermark is affected. Watermark has to be embedded in the invariant transform domain to counteract the synchronization errors.
Commonly used metrics to evaluate image quality are peak- signal-to-noise ratio (PSNR), weighted PSNR (wPSNR), and the Watson just noticeable difference (JND) , structural similarity index measure (SSIM). These metrics can help in achieving the tradeoff between the desired quality and the strength of watermark to be embedded.

More recently, different watermarking techniques and strategies have been proposed in order to solve a number of problems ranging from the detection of content manipulations, to information hiding (steganography), to document usage tracing. The watermarking scheme proposed in this paper is a non-blind watermarking scheme, since it requires the original image to extract the watermark image, is for copyright protection.

This paper focuses on possible attacks against a image watermarking techniques, and work out an effective robust method based on DCT-DWT-SVD that must satisfy the requirements of watermarking scheme. Watermark insertion is done by reordering the cover image and then applying the transforms. The watermark is embedded in the to the middle frequency bands of the DWT of an image. The proposed approach has the following advantages:

1) The extracted watermark is visually recognizable to claim one's ownership;

2) The scheme has multi-resolution characteristics;

3) The embedded watermark is hard to detect by human visual perceptivity;

4) The scheme is very robust against attacks. The transforms used are briefly described in section II.
The proposed hybrid non-blind watermarking scheme is presented in the section III.

The simulation results are illustrated in section IV,
and the concluding remarks are drawn in section V.

2. BASICS OF TRANSFORMS USED FOR WATERMARKING

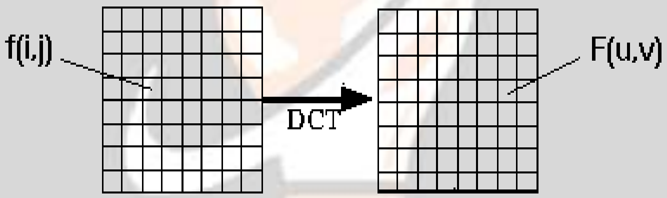
2.1Discrete Cosine transform (DCT)

DCT is widely used in image compression. It is used to linearly transform image to frequency domain. Discrete Cosine Transforms allows to **analyses** complex signal in terms of separate frequency components in a way that is appropriate for compression. frequency components of DCT depending on the correlation in the data.

Compression algorithms operate by breaking data into small blocks. DCT is then applied to each of the blocks, which is how the DCT coefficients are produced. These coefficients are multiplied by a predetermined fixed weight, where higher frequency components use smaller weights. This results in higher frequency components becoming negligible

The general equation for a 2D (*N* by *M* image) DCT is defined by the following equation

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \Lambda(i).\Lambda(j).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] cos\left[\frac{\pi.v}{2.M}(2j+1)\right].f(i,j)$$



The basic operation of the DCT is as follows:

1. The input image is N by M ;
2. f(i, j) is the intensity of the pixel in row i and column j ;
3. f(u, v) is the DCT coefficient in row k1 and column k2 of the DCT matrix.
4. For most images, much of the signal energy lies at low frequencies; these appear in the upper left corner of the DCT.
5. Compression is achieved since the lower right values represent higher frequencies, and are often small - small enough to be neglected with little visible distortion.
6. The DCT input is an 8 by 8 array of integers. This array contains each pixel's gray scale level; 8 bit pixels have levels from 0 to 255.Therefore an 8 point DCT would be:

Where,

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for}\xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

2.2Inverse discrete cosine transform (IDCT)

The IDCT, being the inverse of the DCT. It decodes an image into the spatial domain from a representation of the data better suited to compaction. IDCT-based decoding forms the basis for image and decompression standards. The input to the IDCT comes after the de quantization step and zigzag positioning. An 8x8 block of input values range from -2048 to

2047 and output values in the range -256 to 255. This information is used to reconstruct the image. An original image has no prediction applied and is labeled as an I-picture in the standard. Its pixel values range from 0 to 255.

2.3 Triple Data Encryption Standard (DES)

3DES is a modern variation of DES (Data Encryption Standard), which uses a block of plaintext 64 bits in length, with a 56 bit key. The actual key length equals that of the plaintext. However, the last bit on the right of the key is a parity bit (think of it as padding), and is disregarded as insignificant, which is why 56 bits are the result. (It would be helpful to note that 8 bits equal one byte, you have 8 bytes, each containing 8 bits, equaling a 64 bit block) There were many concerns about the weakness of DES against brute force attacks due to the key length, so 3DES was developed in response to needing a stronger encryption method.

3DES works in much the same way as DES, except that goes through three cycles during the encryption process, using three keys: encryption, decryption, and another encryption. It has a key length of 192 bits (64 bits x 3 keys), but its actual strength is 168 bits (56 bits x 3 keys). This method is three times as strong as DES, yet it also means that it is three times slower because of the triple processing. (Strong Encryption Package, Triple DES Encryption, n.d.)

Encryption using 3DES is represented as C = E(K3, D(K2,E(K1,P))). Similarly, decryption is the same process backwards: P = D(K1,E(K2,D(K3,C))). (Stallings, 2011) So for both algorithms, assume:

P= Plaintext

C = ciphertext

D= decryption function.

E = encryption function

Kx = key ordered by placement in operation

Think of ciphertext as the scrambled message you get after encrypting a message and the key as the scrambler of the plaintext or other ciphertext. To explain in further detail, assume that your key is A = B, B = C, and so on until you reach the end of the alphabet. (This is a sample key, but you can design it however you choose. However, nobody else but the intended recipients should have access to the key, as then it would be too easy to decrypt the message, defeating the purpose of encrypting it.) Your message in plaintext is "Don't forget to drink your Ovaltine". The key scrambles the plaintext, producing the ciphertext "Epou gpshu up esjol zpvs pwbmujof". This process is known as the encryption function. The decryption function would take the ciphertext and key to produce the plaintext message.

To continue with the 3DES algorithm, the innermost parentheses are worked first according to mathematical principles, moving outward. In this example, the innermost parentheses are K1 and P, which indicate the first key combined with the plaintext, and are encrypted (note the "E" directly outside of the first set of parenthesis). This produces the first ciphertext, which is in turn combined with the second key (K2), and decrypted ("D" on outside of second set of parenthesis). The resulting ciphertext is combined with the third key (K3), and encrypted one more time (E on the outside of the first set of parenthesis). The third ciphertext is the final outcome of this operation (indicated by "C").

This follows the encrypt-decrypt-encrypt cycle (EDE):

Encrypt using first key and plaintext to produce first ciphertextDecrypt using first ciphertext and second key to produce second ciphertextEncrypt using second ciphertext and third key to produce final ciphertext

To decrypt the ciphertext, the same operation is performed backwards, as stated in the beginning. The decryption algorithm is stated as P = D(K1,E(K2,D(K3,C))). Recalling the legend in the above example, we are looking to decipher the plaintext, and start with the innermost parenthesis, K3 and C. Starting with the third key (K3), it is combined with the final ciphertext (C) of the encrypted message to perform the first decryption ("D" on outside of innermost set of parenthesis). The resulting ciphertext is then combined with the second key (K2) to encrypt it ("E" on outside of second set of parenthesis), producing the first ciphertext in the example above. The first ciphertext is combined with the first key (K1) to decrypt it a last time ("D" on outside of all parenthesis), producing the original plaintext.

This follows the decrypt-encrypt-decrypt cycle (DED):

Decrypt using the third key and final ciphertext to produce the second cipher text Encrypt using the second ciphertext and the second key to produce the first ciphertextDecrypt using the first ciphertext and the first key to produce the plaintext

One thing to remember is that all three keys should be different. If any of the keys are the same, it would be easier for a hacker to discover the plaintext. For this purpose, several modes of operation were designed for symmetric block ciphers such as 3DES. They include the Electronic Codebook mode (ECB), Cipher Block Chaining mode (CBC), Cipher Feedback mode (CFB), and Counter mode (CTR). While explaining these in detail are out of the scope for this discussion, ECB is a good example of why the same key should not be used. ECB uses the same key for each block of plaintext, and is considered unsecure for long messages. If any two blocks are the same, the ciphertext would be identical. A hacker could decipher the message by method of deduction. (Stallings, 2011)

To summarize, 3DES uses 64-bit symmetric block encryption with three keys, each corresponding to an encryption or decryption function, and follows the EDE cycle to encrypt plaintext, or the DED cycle to decrypt ciphertext. The keys must be kept secret to deter hackers from gaining access to the original plaintext, and should all be independent. On a final note, 3DES is the current standard adopted by the National Institute of Standards and Technology (NIST). It is only a temporary fix until the next generation of encryption is fully integrated, the Advanced Encryption Standard (AES). (Strong Encryption Package, Triple DES Encryption, n.d.)

3.PROPOSED METHOD

The main steps in the proposed hybrid method for non- blind watermarking are summarized below.

3.1 Proposed Method Algorithm

3.1.1 Watermark Insertion

1. The cover image matrix is reordered in a zigzag manner.

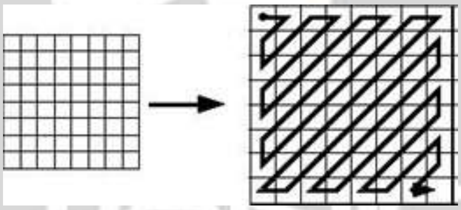


Fig2 shows the zigzag reordering of the image matrix.

2. Apply Discrete Cosine transform (DCT) to the reordered cover image matrix.
3. Apply one-level Haar DWT to the DCT coefficients of the reordered image into four subbands.
4. Apply SVD to LH and HL subbands.

$A^k=U^kS^kV^{kT}$ $k=1,2$

5. Watermark is divided into two parts $W=W^1+W^2$
where W^k denotes half of the watermark.
6. Change the singular values in HL and LH subbands with half of the watermark image and then apply SVD to them, respectively
7. Obtain the two sets of modified DWT coefficients.

i.e., $A^{*k}= U^kS\ ^kV^{kT}$

8.Perform the inverse DWT using two sets of modified DWT coefficients and two sets of non modified DWT coefficients.
9. Perform inverse DCT of the above obtained image matrix.
10. Obtain the watermarked image A_w by reordering the image matrix in a zigzag manner.

3.1.2 Watermark Extraction

1. The watermark image is recorded in a zigzag manner.

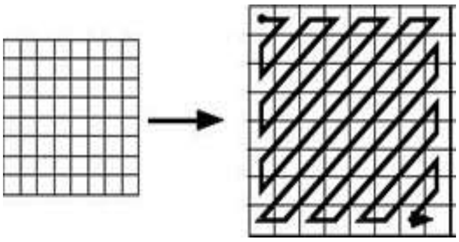


Fig3 zigzag reordering of the image matrix.

2. Apply DCT to the reordered watermarked image and find the DCT coefficients.

3. Use one-level Haar DWT to decompose DCT coefficients into four subbands.

4. Apply SVD to the LH, HL subbands

$^{*k}{}_{W}=U^{*k}S^{*k}{}_{W}V^{*kT}$

5. Compute $B^{*k}=U^{k}{}_{W}(S*^{k}{}_{W})V_{W}{}^{kT}$, $k=1,2$

6. Extract each half of the watermark image from the LH and HL subbands $W^{*k}=(B^{*k}- S^{k})$ /α ,k=1,2

7. Add the results in step 6 to obtain the watermark image.
$W=W^{*1}+W^{*2}$.

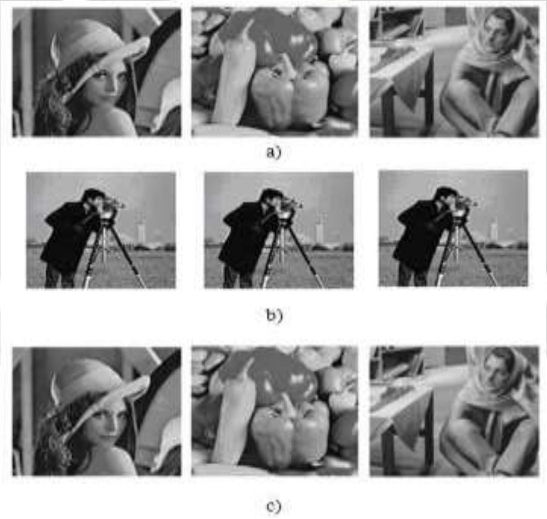


Fig4 Shows the cover images used Lena, peppers and Barbara of size 256 x 256.b) Shows the watermark image used cameraman of size128x128.c) Shows the watermarked images.

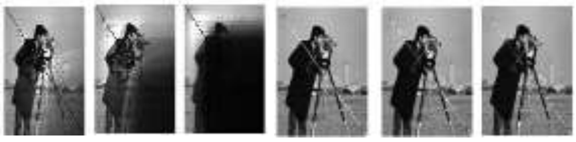


Fig. 6.a)-c) Shows the extracted watermark after JPEG compression. d)-f) Shows the extracted watermark after noising attack.

4.SIMULATION RESULTS

We have tested the proposed watermarking scheme on the popular gray scale test images Lena, Barbara, and Peppers of size 256 x 256 as our cover image and cameraman 128 x 128 as the watermark image.

4.1 Imperceptibility Test

Imperceptibility property must be preserved by watermarking scheme. In order to compare the cover image and watermarked image peak signal to noise ratio (PSNR) is used. The comparison of the PSNR values obtained by implementing the proposed and DWT-SVD method is shown in the table.

Cover image	osed method	DWT-SVD Method
Lena	51.5564	50.2894
Peppers	51.7925	50.4406
Barbara	51.7341	50.9311

Table 1. Comparison of Peak Signal to Noise Ratio

4.1 Robustness Test

The robustness against various attacks is test. The attacks are performed on the watermarked image and watermark is extracted from this watermarked image using the extraction algorithm described in section III. Pearson's correlation coefficient is used to compare the correlation between the original watermark image and the extracted watermark images.

4.1.1 JPEG compression*:*

This scheme can resist JPEG compression up to a quality factor of 30. Fig. 6(a) –(c) illustrates the simulation results after JPEG compression.

Table 2. Pearson's Correlation Coefficient Values of Watermark extracted from JPEG Compressed Watermarked Image

ession factor	posed method		DWT-SVD Method	
	Best	Average	Best	Average
10	0.9844	0.9661	0.9318	0.9083
20	0.9515	0.9286	0.8799	0.8545
30	0.9192	0.8993	0.8487	0.8170

4.2.2Noising Attack:

The Gaussian noise is added to the watermarked image. The Fig. 6(d)-(f) shows the watermarks detected.

Table 3. Pearson's Correlation Coefficient Values of Watermark extracted from Gaussian .

Mean Value	posed method		DWT-SVD Method	
0.8	0.9998	0.9994	0.9998	0.9995
1.2	0.9994	0.9968	0.9957	0.9947
1.6	0.9992	0.9543	0.9786	0.9421

4.2.3 Signal Processing

The watermark can be detected after the watermarked image suffered common signal processing. Fig. 7(a)-(c) shows the simulation results for average filtering or blurring

Table 4. Pearson’s Correlation Coefficient Values of Watermark extracted from Average Filtered Watermarked Image.

opping	**roposed method**		**DWT-SVD Method**	
	Best	**Average**	**Best**	**Average**
columns fi	0.9920	0.9776	0.8678	0.8316
ows from right	0.9886	0.9533	0.8440	0.8316
columns fi	0.9156	0.8979	0.8168	0.7846

5.CONCLUSION

A novel hybrid watermarking scheme based on DCT-DWT- SVD is proposed in this paper. In this method, the watermark is embedded very deep into the cover image since three transform (DCT, DWT, SVD) are taken before embedding the watermark which help in resilience the attacks. This method can be used for copyright protection, tamper detection, fingerprinting, authentication and secure communication. The proposed scheme is robust to JPEG compression, noise adding attacks, contrast adjustment attack, cropping attack, rotation attack and other signal proceeding attacks. Better robustness is obtained at the expense of increased computation time. Experimental results are presented to claim the robustness and correctness of the proposed watermarking process.

6.REFERENCES

[1] Q. Li, C. Yuan, and Y.-Z. Zhong, “Adaptive DWT-SVD Domain Image Watermarking Using Human Visual Model”. In proceedings of 9th International Conference on Advanced Communication Technology.Gangwon- Do,South Korea, pp. 1947-1951.

[2] R. Liu and T. Tan, “An SVD-based watermarking scheme for protecting rightful ownership”. IEEE Trans. Multimedia, vol. 4, no. 1, pp. 121–128, March 2002.

[3] Chih-Chin Lai and Cheng-Chih Tsai.” Digital image watermarking using discrete wavelet transform and singular value decomposition”. IEEE Transactions on instrumentation and measurement, Vol. 59.No. 11.2016.

[4] F. Ahmed and I. S.Moskowitz.”Correlation-based watermarking method for Image Authentication