DCT Moments Based Blind Digital Image Information Hiding And Authentication Scheme Against Various Attacks

Arul Pani Denisha K[1], Dr.K.Madhan Kumar[2], Mrs.C.Rekha[3]

[2, 3]Assistant Professor

[1, 2, 3] PET ENGINEERING COLLEGE

Abstract- *Cyber security attacks on various image data by anonymous unauthorized hackers, with the aim to intercept, corrupt or deny access to the data, have seen a significant increase in recent years. In many homeland security applications, digital information hiding, and image watermarking have seen an increased interest by researchers, given the crucial need of protecting critical information that could threaten our nation security. In data information hiding or watermarking schemes, information is generally hidden either in the spatial domain of the carrier image, or in the carrier image transform such as Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT). In this paper we show, for the first time, a secure, high capacity, authentication, tampering localization, and self-recovery scheme that embeds, with very high imperceptibility, and hides DCT moments of several full gray-scale hidden images (as opposed to binary) and several full gray-scale watermarking images, of the same full size as a given arbitrary carrier host image. The information is embedded into the intensities (as opposed to the DCT moments as is the case of existing classical schemes, in general) of a host carrier image.*

Keywords- Information hiding; image processing; Image water marking; authentication and tampering localization; DCT moments; self-recovery.

I. INTRODUCTION

With cyber security terror threats becoming more frequent, there is a crucial and important need for the development of more secure and robust-to-tampering cyber digital image data information hiding schemes and authentication. Digital watermarking is the process of embedding a logo or other small information at the sending end, called a watermark, in a host image to be detected at the receiver's end. This is for the purpose of image content authentication, copyright protection, or identification.

In data information hiding or watermarking schemes [3] [4] [10] [9] [7] , information is generally hidden either in the spatial domain of the carrier image, or in the carrier image transform such as Discrete Fourier Transform (DFT) [6], Discrete Wavelet Transform (DWT) [7], or Discrete Cosine Transform (DCT) [5].

Each one of these schemes has its own advantages and limitations and its usage is mainly application dependent. In general, one of the biggest limitations of existing image digital watermarking or information hiding schemes stems from the fact that they are limited in the size and the capacity of information that can be embedded in a carrier image, as well as their inability to sustain unauthorized tampering attacks such as image cropping.

Unlike spatial-domain watermarking [10,9,7], frequency domain watermarking schemes, based on frequencies or moments, image transformations including the Discrete Cosine Transform (DCT) and others [17,11,10], are usually popular and compatible to popular image compression standards. In many of these schemes, a given secret digital image is usually converted to its frequency domain moments. These frequency moments are embedded into those of the host image. The inverse Fourier transform is then applied to the latter to form a watermarked image that is ready to be transmitted to the receiving end. Transform-domain methods provide more information embedding and more robustness against many common attacks, but the computational cost is higher than that of spatial-domain watermarking techniques.

The high frequency sub-band of the wavelet decomposed cover image is modified by modifying its singular values. A secret key is generated from the original watermark with the help of visual cryptography to claim the ownership of the image. The ownership of the image can be claimed by superimposing this secret key on the extracted watermark from the watermarked image. The robustness of the technique is tested by applying different attacks and the visual quality of the extracted watermark after applying these attacks is good. Also, the visual quality of the watermarked image is undistinguishable from the original image. In this paper a new robust watermarking technique for copyright protection has been proposed. We applied the singular value decomposition along with the Discrete Wavelet Transform.

1.Paper Main Contributions

In this paper, we propose a scheme combining both information hiding and image watermarking schemes based on DCT transform domain, as further discussed in the next section.

In particular, we show, for the first time, a secure, high capacity and self-recovery scheme that embeds and hides DCT moments, of several full gray-scale hidden images (as opposed to binary) and several full gray-scale watermarking images of the same full size as a given arbitrary carrier host image, into the intensities (as opposed to the DCT moments as is the case of existing classical schemes, in general) of the host carrier image with very high imperceptibility. We show how the proposed algorithm has self-recovery capability to recover most information in case of unauthorized cropping attacks from hackers.

2. Paper Organization paper Objective

The paper is organized as follows: section II, presents the proposed method. In section III we describe and discuss the experimental results, and section IV provides our conclusion and future work.

II. PROPOSED TECHNIQUE

In the proposed scheme, two watermarked images as in [1] are produced and transmitted to achieve the desired objectives and advantages of independency from an arbitrary carrier image, high capacity in both the hidden information and watermark images, high level security, and self-recovery and authentication of the hidden information in case of some tampering attacks. The proposed scheme is capable of hiding the same information in four quadrants of the carrier, by taking advantage of the compactness of the DCT moments to reasonably reconstruct an image from fewer coefficients. In particular, the proposed scheme enables division of the hidden and watermark images into blocks of 16 by 16, takes their DCT moments, but keeps only a few of those moments that are sufficient to reconstruct the original image with reasonable high accuracy.

In particular, here for hiding a watermark and a secret hidden images, of size 256x256 each, into a 256x256 host carrier image, here we only need 28 out of 256 coefficients of a 16x16 block of DCT moments to fully reconstruct the original image. As we show, the idea and aim are to fit enough DCT moments from both the hidden and watermark images into blocks of size 8x8 which are then embedded into 8x8 blocks in a given carrier image. Finally, experimental results on real images are presented to illustrate the efficiency and capabilities of the proposed method, specially to unauthorized cropping attacks. Below, we provide both an embedding and extraction algorithms that are used for the proposed scheme.

A. Proposed Embedding Algorithm

The proposed embedding algorithm, shown in Fig.1, is based on considering 3 images: a carrier image, a watermark image, and a hidden image. The DCT moments of both watermark and hidden images are embedded in intensities of the carrier image with very high transparency.

The watermark image is used to verify the authenticity of the extracted hidden image and localize tampering whenever it occurs. The hidden and watermark images are divided into the same number of blocks of size 16x16 each. The reasons for using blocks are to provide faster reconstruction of watermarked, higher tampering localization accuracy, and higher quality watermarked images. We, then, apply DCT transform on each block.

The compactness of the DCT transform allows us to only choose a few DCT coefficients from each block in order to reconstruct a good quality of hidden image. These coefficients of both hidden and watermark moments are associated with low and medium frequencies and are mostly located in the upper left corner of the image. We discard all but 28 of the 256 DCT coefficients in the upper left of each block. These selected coefficients saved are in an upper triangular and a lower triangular of an arbitrary 8x8 blocks respectively.

We re-arrange all 8x8 blocks into four different quadrants of 256x256 image matrix that result in four redundant 128x128 DCT images of both hidden and watermark images, which results with an image with the same size as the carrier 256x256 image. This image contains reduced DCT moments of the hidden and the watermark images located in four different quadrant of the same image. To add more security to the proposed scheme, the DCT moments within each 8x8 block of the hidden and watermark images are scrambled before being embedded in the intensities of the carrier image blocks.

The DCT moments of each of the scrambled hidden and watermark images are scaled by different mixing weight factors and embedded in the intensities of that of the carrier image blocks as follows.

Watermarked Image1= α*(DCT moments of Watermark image and hidden) + intensities of carrier

Watermarked Image2= β*(DCT moments of Watermark image and hidden) + intensities of carrier

By sending two different watermarked images, this technique provides a blind hiding scheme where the Carrier image is not necessary known at the receiving end. This independency of the carrier image, where secret data is embedded, increases the security and robustness to unexpected attacks, caused by unauthorized hackers.

The advantages of the proposed scheme are: high capacity of hidden data with high imperceptibility due to the added 4- fold redundancy due to the compactness of the DCT, high tampering detection accuracy and image authentication, relatively high quality of self-recovered images in case of cropping tampering, high security, and independency of the scheme on the arbitrary carrier image, for additional security.

B. Proposed Information Extraction Algorithm

As shown in Fig. 2, the watermarked image is processed by the receiver to extract both the watermark and hidden images using the proposed extraction algorithm. The latter requires the watermark image to be present at the receiving end for authentication purposes. After receiving watermarked 1 and 2, both images are divided into blocks of size 8x8. We subtract these blocks in order to make the proposed scheme independent of the carrier image.

Each of these scrambled blocks contains DCT moments of both the watermark and the hidden images. The obtained 256x256 extracted image is divided into four equal quadrant of size 128x128 that contains each the same information of hidden and watermark moments. As a result, each of these four quadrants is used to hide two different images, the hidden and the watermark. The 8x8 blocks of all quadrants are preprocessed to separate watermark moments from hidden moments and save them into 16x16 blocks respectively. The inverse DCT moments (IDCT) are then applied to these blocks to reconstruct the watermark and hidden images back. The purpose of the watermark image in our proposed scheme is to be used to verify authenticity of the extracted images in an attempt to localize any cropping to recover the original image from cyber-attacks.

As explained above, this new watermarking and secret information hiding and authentication technique allows one to embed at least eight different full-scale gray images , of same full size as the carrier, into a single carrier image.

After the extraction process, all four extracted watermark images are tested for any possible attacks such as cropping via their comparison to the original watermark image existing at the receiving's end.

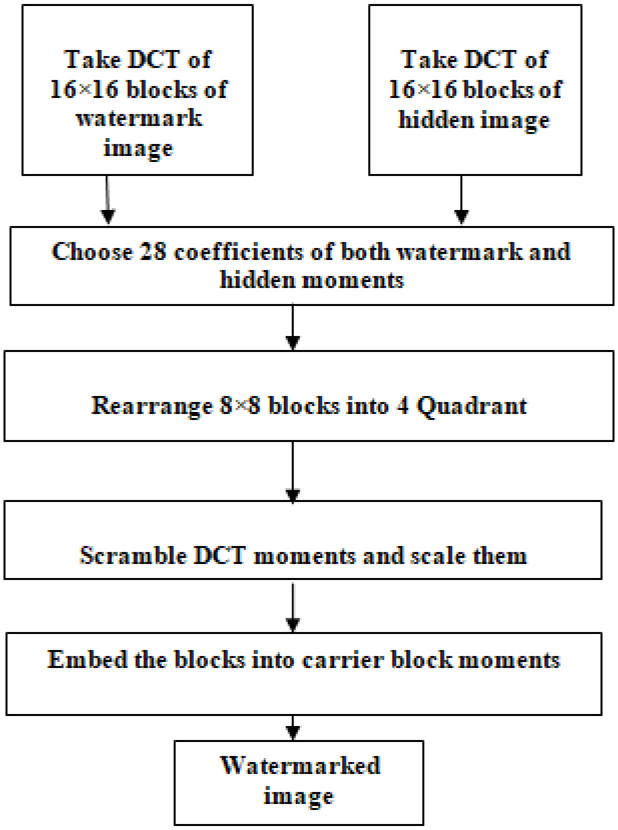

Take DCT of 16×16 blocks of watermark image
Take DCT of 16×16 blocks of hidden image
Choose 28 coefficients of both watermark and hidden moments
Rearrange 8×8 blocks into 4 Quadrant
Scramble DCT moments and scale them
Embed the blocks into carrier block moments
Watermarked image

Fig.1 Flowchart for Information Embedding Algorithm

C. Proposed Embedding Algorithm

The security of the proposed watermarking and information hiding scheme is accomplished here via two techniques. To make the proposed scheme secure, a first and most common technique is used by scrambling the DCT moments of both watermark and the hidden image blocks before they are embedded in the intensities of the carrier image blocks. The scrambling is done using a modulo based algorithm, to increase security (random discontinuities).

The second technique used here to increase security against unauthorized cyber security attacks is accomplished via the independency of the proposed scheme and arbitrary hidden carrier, a newly generated carrier image not publically available is generated every time a hidden secret image needs to be transmitted. At the receiving’s end the hidden secret image can still be extracted since the proposed scheme is a blind scheme, and the carrier does not necessarily have to be available at the receiver’s end .

Sending an arbitrary secret data that is independent of the carrier reduces the risk of a carrier image being recognized and under suspicion of containing hidden information gets hacked or attacked. This above DCT technique of embedding watermark is applied on image by partitioning original image into various blocks. The watermark can be hidden in the digital data either visibly or invisibly. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain. Both the domains are different and have their own pros and cons and are used in unlike scenario. If the signal was not modified during transmission, then the watermark is still present and it can be extracted.

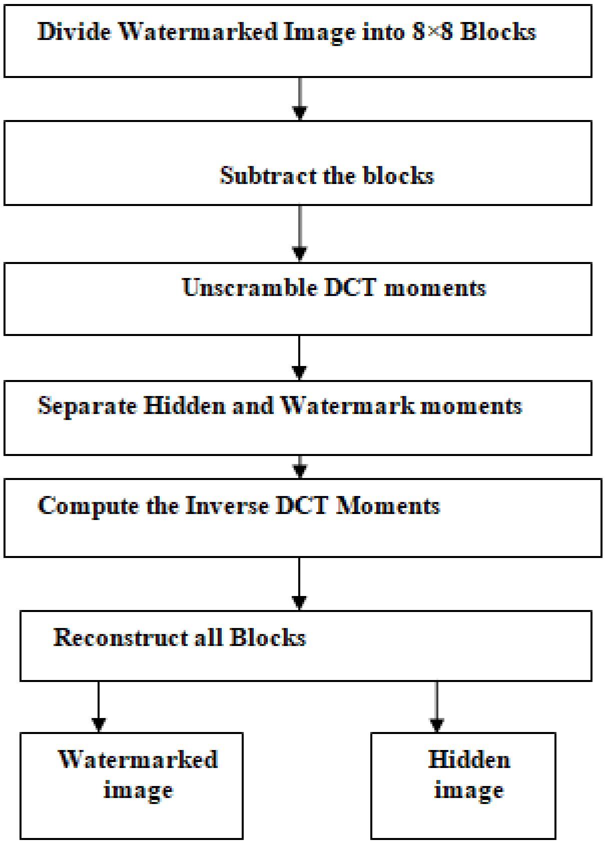
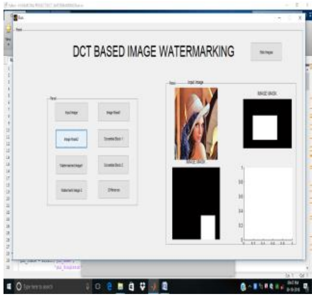

Divide Watermarked Image into 8×8 Blocks
Subtract the blocks
Unscramble DCT moments
Separate Hidden and Watermark moments
Compute the Inverse DCT Moments
Reconstruct all Blocks
Watermarked image
Hidden image

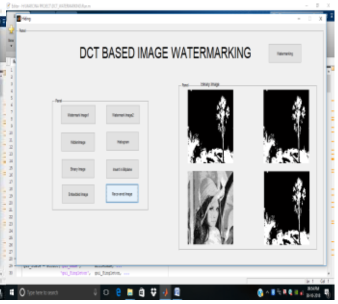
Fig.2 Flowchart for Information Extracting Algorithm

III. EXPERIMENTAL RESULTS

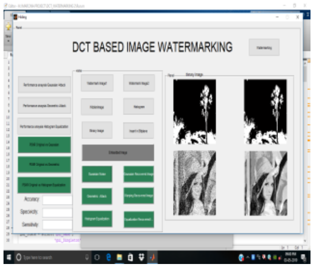
In this section, we discuss the results obtained from applying the proposed watermarking, information hiding and authentication scheme on three different grey images: carrier image, watermark image, and hidden image. In particular, Figure (a) shows the input image and the two types of masking for inserting into carrier image. Figure (b) shows the embedding image & recovered image and Figure (c) shows the attacked image by Gaussian noise.

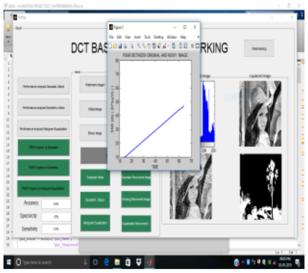
Figure (d) shows the PSNR value between original image and noisy image. Figure (e) shows the attacked image by Geometric distortion . Figure (f) represents the PSNR value between original image and distorted image. Figure (g) shows the attacked image by histogram equalization. Figure (h) represents the PSNR value between original image and equalized image.



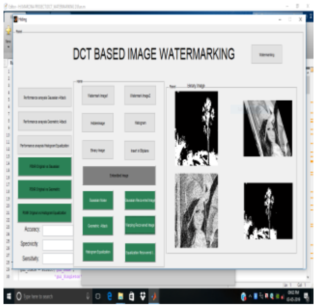


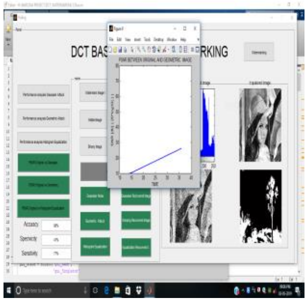
(a) Input image & image masking (b) Embedding image & Recovered image



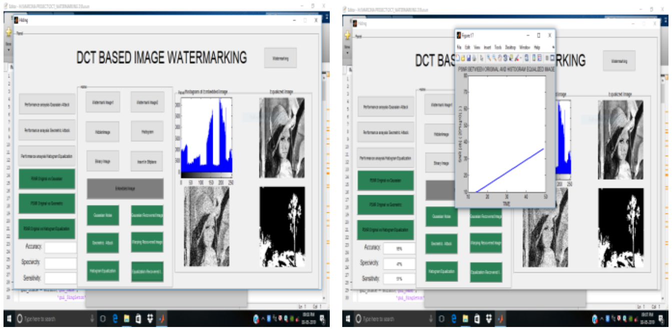


(c)Attacked Image by Gaussian Noise (d) PSNR Value Between Original Image and Noisy Image





(e) Attacked Image by Geometric Distortion (f) PSNR Value Between Original Image and Distorted Image



(g)Attacked image by histogram equalization (h) PSNR value between original Image and equalized image

Fig-3: Some experimental results of the proposed algorithm. The proposed scheme is based on hiding DCT moments of a hidden image and an authentication watermark image into intensities of a carrier image. This scheme is a blind scheme for it is independent of the arbitrary and changing carrier image for security.

Image Enhancement attacks are convolution operations that desynchronize the watermark information in an image. These attacks include histogram equalization, sharpening, smoothing, median filtering and contrast enhancement. A watermark system is said to be secure, if the hacker cannot remove the watermark without having full knowledge of embedding algorithm, detector and composition of watermark. A watermark should only be accessible by authorized parties. This requirement is regarded as a security and the watermark is usually achieved by the use of cryptographic keys. The effect of equalization on watermarked images is greatly reduced by proper selection of algorithm. The experimental results show that the algorithm is robust to enhancement attack.

IV. CONCLUSIONS

A new secure, high capacity, and most importantly self-recovery capable watermarking, secret information hiding and authentication scheme based on DCT moments was successfully tested and verified in this paper. In this proposed scheme, DCT moments of two arbitrary gray images, up to the same size as the one of an arbitrary carrier image, are hidden with high imperceptibly in the intensities of the carrier image. To make the scheme even more secure, we make the carrier image unknown at the receiving end which allows for independency of the watermark and hidden images of the carrier image. Another aspect of security is applied via scrambling the DCT moments of the hidden and the watermark images blocks before embedding them in the intensities of the carrier image. Watermarked images are affected by various attacks such as removal, noise and rotation. These attacks destroy the inserted watermark, so that the copyright problem may arise. All the attacks are the threats for every watermarking algorithms and techniques. They degrade or destroy the watermark information. So the watermarking algorithm should be as robust as it can be resist against these attacks. MATLAB is scientific tool by which researchers can easily tests the strength of any particular algorithm against these attacks. The described DCT algorithm had a capability of resistance against these attacks.

REFERENCES

[1] Suzan Al-Shoura, D.B. Megherbi, "Comparative of Zernike and Tchebichef Moments ForImage tampering Detection Sensitivity and Watermak Recovery", Proceedings of the IEEE International Conference on Homeland Security, MA, June 2008.

[2] S. El Shoura, D. B. Megherbi, "High Capacity Blind Information Hiding Schemes Using Tchebichef Moments", IEEE International Conference on Future Computer and Communications (IFCCC), May 2010.

[3] Y. Xiang, D. Peng, I. Natgunanathan, and W. Zhou, "effective pseudonoise sequence and decoding function for imperceptibility and robustness enhancement in time spread scho based audio watermarking, "IEEE Trans. on Multimedia, Vol. 13, no. 1, pp. 2-13, Feb.2011.

[4] Susan Elbardy, Yong Xian, TianruiZong, IymkaranNatgunanathan, "A new interpolation error expansion based reversible watermarking algorithm considering the human visual system", Communications (ICC) 2014 IEEE international Conference on, pp. 890-900, 2014.

[5] Shahin Shaikh, ManjushaDeshmukh," Digital Image Watermarking in DCT Domain", International Journal of Emerging Technology and Ad-vanced Engineering ISSN 2250- 2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013

[6] R. K. Sharma and S. Decker, "Practical Challenges for Digital Watermarking Applications", IEEE Fourth Workshop on Multimedia Signal Processing, pages: 237-242, Oct. 3-5, 2001.

[7] L. Zhang, G. Qian, W. Xiao, and Z. Ji, "Geometric Invariant Blind Image Watermarking by Tchebichef Moments," Optics Express, vol. 15, no. 5, pp. 2251 – 2261, March 2007.

[8] S.M. Elshoura and D.B. Megherbi, "Noise Analysis and Reconstruction Accuracy for Tchebichief Moments," to appear in the Proceedings of IEEE Southeastcon., 2008.

[9] M. Pawlak and Y. Xin, "Robust Image Watermarking: An invariant Domain Approach," Proceedings of IEEE Canadian Conference on Elec. & Computer Eng., 2002.

[10] A.Nikolaidis, S.Tsekeridou, A.Tefas, and V. Solachidis, "A Survey on Watermarking Application Scenarios and

Related Attacks", Proceedings of 2001 international conference on Image Processing, vol. 3, pages: 991-994, Oct. 7-10, 2001.