International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Blind Digital Image Information Cloaking and Authentication Scheme Using DCT

R. V. S. Harish[1], D. Swathi, G. Lavanya[2], D. Pavan kumar[3], B. Naveen, B.Raja[4]
[1, 2, 3, 4] *Department of Electronics and Communication Engineering, St. Ann's College of Engineering & Technology, Chirala, A.P., India*

Abstract: ***Cyber security attacks on various image data by anonymous unauthorized hackers, with the aim to intercept, corrupt or deny acess to the data, have seen a significant increase in recent years. Secure digital image communications on the internet and via networked systems is important in many multimedia commercial, government, and defense applications.. In many homeland security applications, digital information cloaking, 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 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 secret images (as opposed to binary) and several full gray-scale watermarking images, of the same full size as a given arbitrary carrier/target 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/target image. We show how the proposed algorithm has self-recovery capability to recover most lost information in case of unauthorized cropping attacks from hackers. The objective is the ability, via a blind scheme where the carrier/target not required/known at the receiving end.***

Keywords:-Information cloaking; image processing; Image watermarking; authentication and tampering localization; DCT moments; self-recovery.

I. INTRODUCTION

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 cloaking or watermarking schemes, information is generally secret either in the spatial domain of the carrier/target image, or in the carrier/target image transform such as Discrete Fourier Transform (DFT)], Discrete Wavelet Transform (DWT), or Discrete Cosine Transform (DCT). 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 cloaking schemes stems from the fact that they are limited in the size and the capacity of information that can be embedded in a carrier/target image, as well as their inability to sustain unauthorized tampering attacks such as image cropping. computational cost is higher than that of spatial-domain watermarking techniques. Additionally, a self recovery capability of full gray-scale secret images, after a cropping attack, is currently very challenging and an area of high research interest. To our knowledge, there is no scheme or work in the literature where several full-gray-scale images, of the same size as the carrier/target, are secret into an arbitrary carrier/target image, with high imperceptibility/transparency, while exhibiting robustness to cropping with relatively high accuracy of self-recovery.

II. PROPOSED SCHEME

In the proposed scheme, two watermarked images as in are produced and transmitted to achieve the desired objectives and advantages of independency from an arbitrary carrier/target image, high capacity in both the secret information and watermark images, high level security, and self-recovery and authentication of the secret information in case of some tampering attacks. Below, we provide both an embedding and extraction algorithms that are used for the proposed scheme.

A. Embedding Algorithm

The proposed embedding algorithm, shown in Fig.1, is based on considering 3 images: a carrier/target image, a watermark image, and a secret image. The DCT moments of both watermark and secret images are embedded in intensities of the carrier/target image with very high transparency. The watermark image is used to verify the authenticity of the extracted secret image and localize

tampering whenever it occurs. The secret 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 secret image. These coefficients of both secret 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 secret and watermark images, which results with an image with the same size as the carrier/target 256x256 image. This image contains reduced DCT moments of the secret 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 secret and watermark images are scrambled before being embedded in the intensities of the carrier/target image blocks. The DCT moments of each of the scrambled secret and watermark images are scaled by different mixing weight factors and embedded in the intensities of that of the carrier/target image blocks as follows.

Watermarked Image1= α*(DCT moments of Watermark image and secret) + intensities of carrier/target**.**

Watermarked Image2= β*(DCT moments of Watermark image and secret) + intensities of carrier/target.

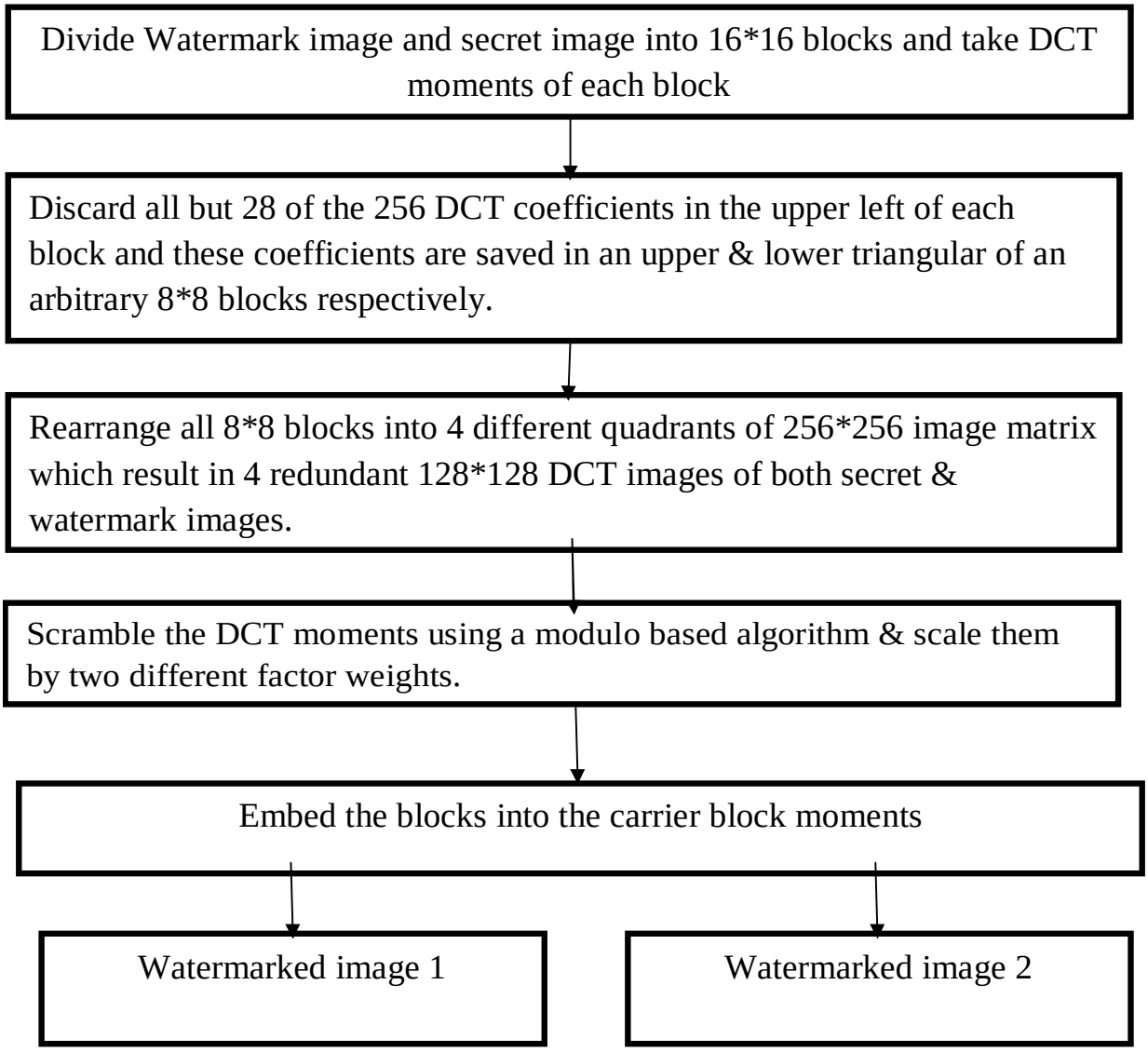

Fig a) Information Embedding Algorithm

By sending two different watermarked images, this technique provides a blind cloaking scheme where the Carrier/target image is not necessary known at the receiving end. This independency of the carrier/target 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 secret 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/target image, for additional security.

B. Extraction Algorithm

As shown in Fig. 2, the watermarked image is processed by the receiver to extract both the watermark and secret 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/target image. DCT moments within each 8x8 block are unscrambled the same way they are scrambled at the sender's end, using a user defined algorithm, known also at the receiver end. Each of these scrambled blocks contains DCT moments of both the watermark and the secret images. The obtained 256x256 extracted image is divided into four equal quadrant of size 128x128 that contains each the same information of secret and watermark moments.

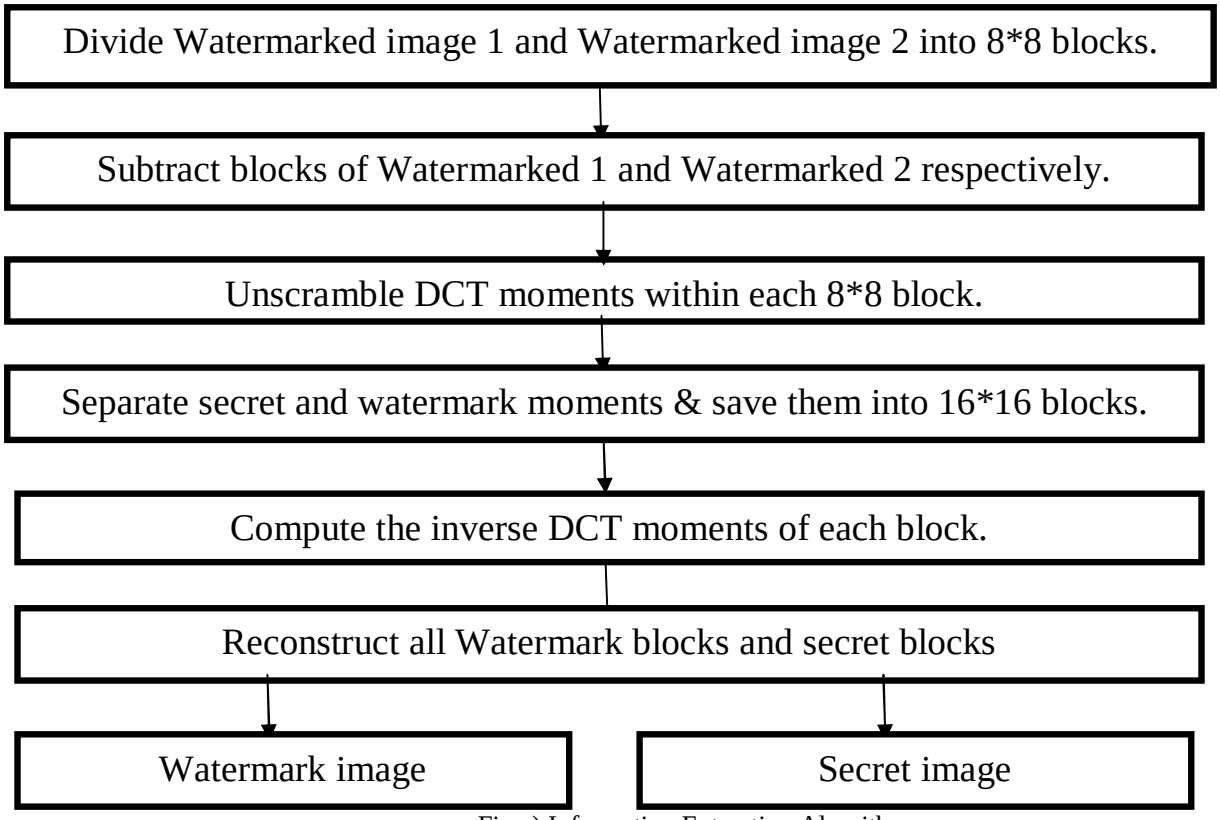

Fig a) Information Extracting Algorithm

As a result, each of these four quadrants is used to hide two different images, the secret and the watermark. The 8x8 blocks of all quadrants are preprocessed to separate watermark moments from secret moments and save them into 16x16 blocks respectively. The inverse DCT moments (IDCT) are then applied to these blocks to reconstruct the watermark and secret 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 cloaking and authentication technique allows one to embed at least eight different full-scale gray images, of same full size as the carrier/target, into a single carrier/target 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.

At the receiving's end the secret image can still be extracted since the proposed scheme is a blind scheme, and the carrier/target does not necessarily have to be available at the receiver's end . Sending an arbitrary secret data that is independent of the carrier/target reduces the risk of a carrier/target image being recognized and under suspicion of containing secret information gets hacked or attacked.

III. EXPERIMENTAL RESULTS

In this section, we discuss the results obtained from applying the proposed watermarking, information cloaking and authentication scheme on three different jpeg images: carrier/target image, secret image, and watermark image.

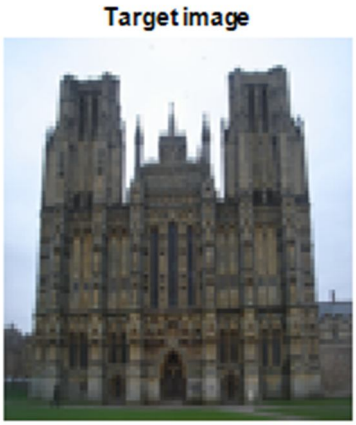

Fig (i)

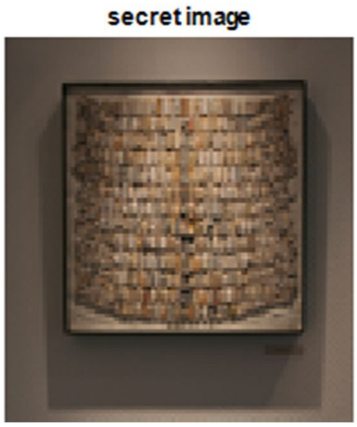

Fig (ii)

Fig (iii)

Fig (iv)

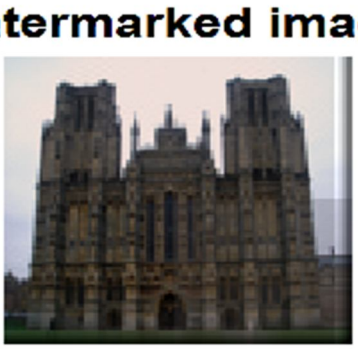

Fig (v)

Figures (iv) and (v) show the watermarked image 1 and the watermarked image 2 after DCT moments of watermark and secret images being embedded in the intensities of that of carrier image.

Fig (vi)

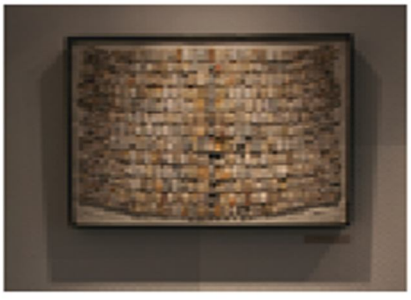

Fig (vii)

Figures (vi) and (vii) shows each respectively an automatic self-recovered-to-cropping extracted watermark image and an automatic self-recovered-to-cropping secret image.

IV. CONCLUSION

A new secure, high capacity, and most importantly self-recovery capable watermarking, secret information cloaking 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/target image, are secret with high imperceptibly in the intensities of the carrier/target image. To make the scheme even more secure, we make the carrier/target image unknown at the receiving end which allows for independency of the watermark and secret images of the carrier/target image.

Another aspect of security is applied via scrambling the DCT moments of the secret and the watermark images' blocks before embedding them in the intensities of the carrier/target image. The scheme is also tested against cropping attacks, its high capacity while keeping high transparency, and self recovery ability by cloaking 8 full-scale gray images of same size as the carrier/target, in four quadrant of the same carrier/target image. The results showed that when there are no attacks, the secret images were extracted with high accuracy and quality. In the case of cropping, the scheme was capable of accurately localizing the cropped areas, and of self-recovery of the extracted secret information.

REFERENCES

[1] 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.

[2] Varghese, Justin; Subash, Saudia; BIN Hussain, Omer; Nallaperumal, Krishnan; Ramadaa SAADY, Mohammed; SAMIULLA KHAN, Mohamed. Turkish Journal of Electrical Engineering & Computer Sciences. 2016, Vol. 24 Issue 5, p3432-3447. 16p. DOI: 10.3906/elk-1409-12.

[3] R. Mukundan, CISST01 International Conference, Discrete vs. Continuous Orthogonal Moments for Image Analysis, (2001).

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

[5] Ruchira Naskar and R. S. Chakraborty, ―Reversible Digital Watermarking: Theory and Practices‖, Morgan Claypool, USA, ISBN: 978-1627053150 .

[6] Tanmoy Sarkar, Sugata Sanyal, "Reversible and Irreversible Data Hiding Techniques‖ in arxiv.org, arXiv: 1045.2684, 2014 .

[7] F. Battisti, M. Carli, A. Neri, K. Egiaziarian, ―A Generalized Fibonacci LSB Data Hiding Technique‖, IEEE 3rd International Conference on Computers and Devices for Communication (CODEC-06) TEA, Institute of Radio Physics and Electronics, University of Calcutta, December 18-20, 2006.

[8] Sandipan Dey, Ajith Abraham, Sugata Sanyal, ―An LSB Data Hiding Technique Using Natural Numbers‖, Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP 2007. Third International Conference, Kaohsiung, Vol.2, 2007, pp. 473-476. For i, j=0 For i, j ≠0

[9] M. Nosrati, R. Karimi, H. Nosrati, and A. Nosrati, ―Embedding stego-text in cover images using linked list concepts and LSB technique‖, Journal of American Science, Vol. 7, No. 6, 2011, pp. 97-100

[10] . Ni, Y. Q. Shi, N. Ansari and W. Su, ―Reversible data hiding,‖ IEEE Transactions on Circuits and Systems for Video Technology, Vol.16, No.3, pp. 354-362, 2006