International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 10 161 - 164

# Survey on 2D-DCT Based Image Watermarking with High Implanting Limit and Robustness

K. Namrata[1],
M.E (CSE) Student,
Tagore Institute of Engineering and Technology, Salem, India.

R. C. Karpagalakshmi[2],
M. Tech, Assistant Professor/CSE,
Tagore Institute of Engineering and Technology, Salem, India.
*karpagalakshmirc@gmail.com*

Dr. D. Tensing[3]
Director, School of Civil Engineering, Karunya University, Coimbatore, India
*dtensing@rediffmail.com*

***Abstract*** **-** The proposed strategy displays a novel rank-based image watermarking. In watermark installing process, the host picture is separated into squares, trailed by 2-D Discrete Cosine Transform (DCT). For every picture block, a mystery key is produced utilizing RFC 2898, which incorporates techniques for making a key and introduction vector (IV) from a secret word and salt. The inserting of watermark bits is completed by adjusting the arrangement of DCT coefficients utilizing a rank-based installing rule.The created mystery key is imparted to the receiver while sending the picture.On watermark location process, with the utilization of accessible mystery key, the watermarked bits are distinguished and are extricated inview of positions of discovery lattices. The pictures transferred for general visibility is shown by DCT which assumes a vital part in keeping up the measure of the picture amid this procedure. Since the proposed watermarking strategy just uses two DCT coefficients to shroud one watermark bit, high installing limit can be accomplished. Also, this strategy is free of host signalinterference. This sought component andthe use of a blunder cushion in watermarkinserting can bring about high vigor against assaults. Hypothetical examination and trial results will exhibit the adequacy of the proposed strategy.

***Index Terms*** **-** *2d-DCT watermarking, RFC 2898, Robustness.*

*****

## I. INTRODUCTION

With the quick development of correspondence systems and advances in interactive media handling advances, sight and sound theft has turned into a significant issue. In an open system environment, advanced watermarking is a promising innovation to handle sight and sound information theft. In advanced watermarking, the watermark information (for example, distributer data, client identity, file exchange/downloading records and so forth) are covered up into the genuine sight and sound article without influencing its typical usage. When important, the proprietors or law requirement offices can remove the watermark information by utilizing a mystery key to follow the wellspring of unlawful dissemination. While advanced watermarking can be connected to different mixed media information, for example, sound, picture and video.

This paper concentrates on picture watermarking. With regards to picture watermarking, imperceptibility, robustness [8], implanting limit and security [9] are of essential concerns. As such, different picture watermarking plans have been accounted for in the writing and large portions of them were based upon strategies identified with histogram [3], minute[3][6], spatial element areas[1], spread range (SS)[4] and quantization[2]. In numerous applications, for example, undercover correspondence, high inserting limit is desired, while strength against geometric assaults is not fundamentally concerned[9].

The proposed technique, introduces a novel rank-based picture watermarking scheme to altogether increment inserting capacity while keeping up agreeable intangibility and robustness against basic assaults. At the watermark implanting process, the 2-D Discrete Cosine Transform (DCT) [5]is connected to every picture block to get the equivalent DCT coefficients. A mystery key is utilized to arbitrarily pick an arrangement of DCT coefficients suitable for inserting watermark. The installing of watermark bits is done by changing the arrangement of DCT coefficients using a rank-based inserting principle, where a blunder cushion is also utilized to manage the mistakes brought on by assaults. The watermark recognition process can figure the DCT coefficients from the got picture and after that develop the detection matrices utilizing the same mystery key[5]. The inserted watermark bits can be removed by checking the positions of the detection matrices. Contrasted and the current picture watermarking methods[5][3], the proposed strategy can have much higher embedding capacity. In the meantime, it has high perceptual quality and is strong against normal assaults.

## II LITERATURE SURVEY

[3][5] TianruiZong, Yong Xiang, Song Guo, Wanlei Zhou, GlebBeliakov have proposed a novel picture watermarking

technique to manage the cropping and random bending assaults, and in addition to the other basic assaults. The installing procedure of the host picture is done by a Gaussian low-pass channel. At that point a mystery key is utilized to haphazardly choose various grey levels and the histogram of the separated picture with these chosen grey levels is built. After that, a histogram-shape-related index is introduced to pick the pixel bunches with the most elevated number of pixels and a protected band is built between the picked and non-picked pixel bunches. A watermark installing plan is proposed to embed watermarks into the picked pixel bunches. The utilization of the histogram-shape-related list and safe band brings about great robustness. Additionally, a novel high-recurrence segment modification mechanism is likewise used in the inserting plan to facilitate enhance robustness. At the disentangling end, in view of the accessible mystery key, the watermarked pixel groups are recognized and watermarks are removed from them.

[1] M. Kim, D. Li and S. Hong have proposed a powerful advanced picture watermarking techniques based on the various change strategies to be specified as , Discrete Wavelet Transform (DWT) and Discrete Fractional Random Transform (DFRNT). At that point, it receives a two-dimensional (2D) barcode for concealing data and applies the piece code encoding and creates a watermark through them. The created watermark picture is inserted into DWT-DFRNT utilizing quantization method as a part of request to guarantee strength and indistinctness of the watermark. Exploratory results exhibit that our proposed calculation has enhanced the extraction execution by precisely removing the shrouded data in the 2D standardized tag from the distinguished watermark. Likewise, joining the double change strategy, DWT and DFRNT, has enhanced the imperceptibility and robustness of the watermark against essential picture flag handling assaults.

[2]Myasar Mundher, Amjad Rehman, Dzulkifli Muhamad, Tanzila Saba and Firdous Kausar have proposed computerized pictures watermarking way to deal with the management of the proprietorship and genuine confirmation. To secure the scholarly assets of pictures, sound and recordings, watermark W is changed over into a succession of bits and keeping in mind that the end goal that is used to encode the watermark, arrangement of size R is chosen arbitrarily. Also, a pseudo arbitrary number is created to compute pixels for determination key generation. At last, 2-level Discrete Slanlet Transform (DST) on the host picture is connected in order to partition it into Red, Green and Blue channels. The outcomes in this way delivered from proposed philosophy show robustness against the current cutting edge. Further, the proposed approach adequately removes the watermark without the first pictures.

[4]Jyothi B and Ramesh Kumar H K have proposed a novel multi-bearer/signature iterative generalized least squares (M-IGLS) center method to look for the obscure information that is covered up in the hosts by means of multi-transporter spread range implanting procedure. Neither the first host nor the implanting transporters are thought to be accessible. Test is considered on the pictures to demonstrate that the created calculation can accomplish recuperation likelihood of blunder near what might be achieved with the known installing bearers and the host autocorrelation lattice.

[5]TianruiZong and Yong Xiang have proposed a novel rank-based technique for picture watermarking. In the watermark implanting process, the host picture is partitioned into pieces, trailed by 2-D discrete cosine transform (DCT). For every picture block, a mystery key is utilized to haphazardly after choosing an arrangement of DCT coefficients which is appropriate for watermark implanting. Watermark bits are embedded into a picture obstruct by changing the arrangement of DCT coefficients utilizing a rank-based installing standard. In the watermark discovery process, the comparing recognition matrices are framed from the received picture utilizing the mystery key. After a while, the watermark bits are separated by checking the positions of the discovery lattices.

Since the proposed watermarking technique just uses two DCT coefficients to shroud one watermark bit, it can accomplish high implanting limit. In addition, our strategy is free of host signal interference. This craved component and the utilization of a blunder cushion in watermark installing result in high strength against assaults. Hypothetical examination and trial comes about exhibiting the adequacy of the proposed strategy.

## III PROPOSED SYSTEM

From this comparative study, it has been analyzed that water marking can be further enhanced. In this paper, introduce a novel rank-based picture watermarking method to altogether increment installing capacity while keeping up attractive indistinctness and robustness against normal assaults. In the proposed technique, the 2-DDiscrete Cosine Transform (DCT)[5] is connected to every picture block to acquire the comparing DCT coefficients. A mystery key is utilized to arbitrarily pick an arrangement of DCT coefficients suitable for installing watermarks. The installing of watermark bits is done by changing the arrangement of DCT coefficients using a rank-based implanting guideline, where a mistake cradle is also utilized to manage the blunders brought on by assaults.[5] At the watermark location end, then process the DCT coefficients from the got picture and afterward build the detection matrices utilizing the same mystery key. The implanted watermark bits can be removed by checking the positions of the detection matrices. Contrasted and the current picture watermarking methods, the proposed technique has much higher embedding capacity. In the meantime, it has high perceptual quality and is strong against regular assaults. [5] The unrivalled performance of our strategy is broke down in principle and showed by

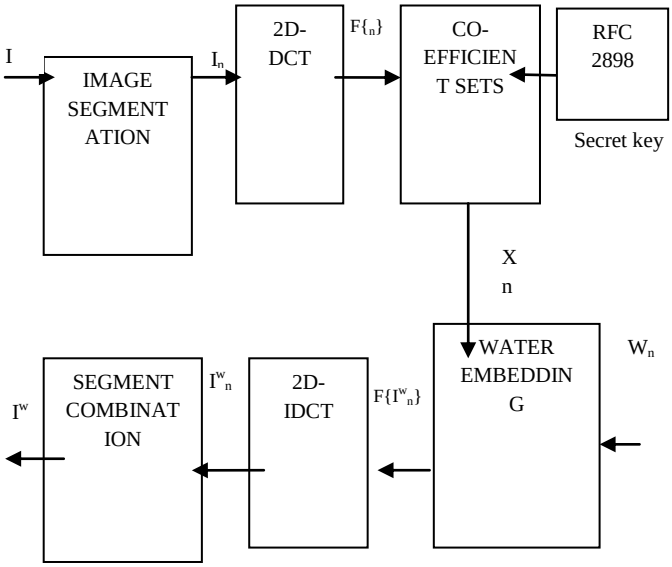
simulation results. Then using encrypt the mystery message by means of Password Based Encryption (PEB) calculation to secure the clients mystery messages. Also, add that scramble message to watermark of every single split pictures. The proposed picture watermarking strategy made out of two sections:

*A. Watermark Embedding Process*

[5]In each block, it utilizes a mystery key to haphazardly choose 2K reasonable DCT. RFC 2898, Implements secret key based key deduction usefulness and then applies PBKDF2, by utilizing a pseudo-arbitrary number generator in light of HMACSHA1.

RFC 2898 incorporates techniques for making a key and introduction vector (IV) from a secret key and salt by executing PBKDF2, a watchword based key determination capacity, to infer keys utilizing a pseudo-arbitrary capacity that permits keys of for all intents and purposes boundless length to be created. In a secret word based key determination work, the base key is a watchword and alternate parameters are a salt worth and an emphasis tally.

HMACSHA1 is a sort of keyed hash calculation that is built from the SHA1 hash work and utilized as a HMAC, or hash-based message verification code. The HMAC procedure blends a mystery key with the message information, hashes the outcome with the hash capacity, blends that hash esteem with the mystery key once more, and after that applies the hash work a second time. The yield hash is 160 bits long.




*B. Watermark Detection Process*

In the proposed watermarking technique, watermark identification is executed by checking the positions of the recognition grids, which makes our strategy free of host signal interference(HSI)[5].

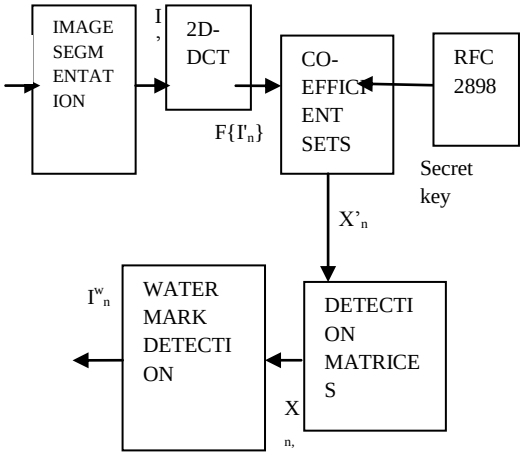



Fig:1: Watermark Detection Process

This component is vital for accomplishing high recognition rate. In addition, the mistake support utilized in the implanting procedure further upgrades the location execution as it can, to an expansive degree, endures the blunders forced by the assaults.

## V CONCLUSION

From this literature survey, it is found that the techniques supporting multiple tables are not very efficient. Here proposed a novel technique for image watermarking in the DCT space. The proposed watermarking method has some attractive elements. Firstly, our strategy can use as meager as two DCT coefficients to embed one watermark bit. The discrete cosine transform (DCT) isolates the picture into parts of contrasting significance. Besides, it is free of HSI. Thirdly, it can extensively endure the mistakes created by attacks. In RFC2898, multiple emphasis (1000 default) moderate down secret word speculating assaults dissimilar to AES. The first highlight prompts high installing limit. The second and third components make the proposed technique powerful against common assaults. The predominant execution of the new method will be examined hypothetically in point of interest and exhibited by simulation comes about.

## REFERENCES

[1] M. Kim, D. Li and S. Hong," A Robust Digital Watermarking Technique for Image Contents based on DWT-DFRNT Multiple Transform Method",International Journal of Multimedia and Ubiquitous Engineering,Vol.9, No.1 (2014), pp.369-378.

[2] MyasarMundher, Dzulkifli Muhamad, AmjadRehman, Tanzila Saba and FirdousKausar," Digital Watermarking for

Images Security using Discrete SlantletTransform",Applied Mathematics & Information Sciences,An International Journal 8, No. 6, 2823-2830 (2014).

[3] TianruiZong, Yong Xiang, IynkaranNatgunanathan, Song Guo, Wanlei Zhou and GlebBeliakov," Robust Histogram Shape Based Method for Image Watermarking",IEEE Transactions on Circuits and Systems for Video Technology.

[4] Jyothi B1. Rameshkumar H K,"Extracting Spread-Spectrum Hidden Data from Digital Media",International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization), Vol.3, Issue 4, April 2015.

[5] TianruiZong, Yong Xiang, Song Guo and Yue Rong," Rank-Based Image Watermarking Method with High Embedding Capacity and Robustness",Vol.4,2016,Digital Object Identifier 10.1109/ACCESS.2016.2556723.

[6] ShivaniKashyap, Mandeep Singh Saini," Histogram Based Watermarking Using Entropy Technique In Digital Images",International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 4, Issue 3, March 2015 666 ISSN: 2278 – 909X

[7] Shaheen Begum," Invariant Image Watermarking Based on Statistical Features in the Low-Frequency Domain", Volume No: 3 (2016), Issue No: 2 (February) International Journal & Magazine of Engineering, Technology, Management and Research.

[8] Kaiser J. Giri, Mushtaq Ahmad Peer and P. Nagabhushan," A Robust Color Image Watermarking Scheme Using Discrete Wavelet Transformation", I.J. Image, Graphics and Signal Processing,2015, 1, 47-52 Published Online December 2014 in MECS.

[9] Po-Chyi Su and Yu-Chuan Chang," A Geometrically Resilient Digital Image Watermarking Scheme Based on SIFT and Extended Template Embedding", INTERNET 2012 : The Fourth International Conference on Evolving Internet, ISBN: 978-1-61208-204-2.

Table.I-Represents the comparative study of various approaches regarding watermarking in variousaspects.

TABLE I COMPARATIVE STUDY

| AUTHOR | YEAR | TITLE | TECHNIQUES | RESULT |
|---|---|---|---|---|
| TianruiZong, Yong Xiang Yue Rong, | 2016 | Rank-Based Image Watermarking Method with High Embedding Capacity and Robustness | 2-D Discrete CosineTransform , RFC 2898, Password-Based Key Derivation Functionality, | Free of HIS<br>High embedding capacity<br>High robustness |
| Jyothi, Rameshkumar H K | 2015 | Extracting Spread-Spectrum Hidden Data from Digital Media | Multi carrier/signature iterative generalized least-squares (M-IGLS) | Low time consumption<br>High attack resistance |
| M. Kim,D. Li, S. Hong | 2014 | A Robust Digital Watermarking Technique for Image Contents based on DWT-DFRNT Multiple Transform Method | Discrete Wavelet Transform (DWT), Discrete Fractional Random Transform (DFRNT) | Robust against Image compression and noise adding<br>Embedded 2D barcodes as the watermarks could be perfectly restored |
| TianruiZong, Yong Xiang Song Guo, Wanlei Zhou, GlebBeliakov, | 2014 | Robust Histogram Shape Based Method for Image Watermarking | Gaussian low-pass filter Histogram shape related index | Improved to compensate the side effects of Gaussian filtering<br>Increased robustness to geometric attacks |
| MyasarMundher,Dzulkifli Muhamad AmjadRehman, Tanzila Sabaand FirdousKausar | 2014 | Digital Watermarking for Images Security using Discrete Slantlet Transform | Discrete Slantlet Transform (DST) | Ensures the imperceptibility and robustness |