Digital picture watermarking technique for security applications

B Swapna, M Kamalahasan, S Srinidhi, S Sowmiya, S Vasanth, and P Sri Divyabharathi
Dr MGR Educational and Research Institute, Chennai, India

Email: swapna.eee@drmgrdu.ac.in

Abstract: Digital picture watermarking is employed to stay secret the proprietary info as a watermark within a digital image, to spot the possession. This method has relevancy to any or all pictures. Separate trigonometric function transform (DCT) is employed before inserting the watermark within the host image. The host picture is isolated into 8×8 non-covering hinders preceding DCT application, and therefore the watermark bit is inserted by dynamic distinction between DCT coefficients of contiguous squares. Arnold transform is employed even so disorderly encoding to feature 2-fold block safeguard to the watermark. 3 distinctive variations of the planned calculation are tried and stone-broke down. The reenactmen results demonstrate that the planned set up is powerful to the overwhelming majority of the image making ready tasks like JPEG pressure, honing, trimming, middle separating, and so on. To approve the proficiency of the planned technique, the recreation results are contrasted and sure condition of workmanship systems. The examination results represent that the planned set up performs higher as so much as power, security and imperceptivity. Given the advantages of the planned set up, it alright could also be used in applications like e-social insurance and telemedicine to smartly hide out electronic eudemonia records in therapeutic footage.

Keywords: DCT, Chaotic transform, Arnold transform, watermarking.

1. INTRODUCTION

In the domain of mechanized watermarking, picture watermarking dominantly has entranced a lot of eagerness for the investigation arrange. The major part of the assessment work is resolved to picture watermarking when stood out from sound and video. A bit of the reasons is depicted underneath. The test pictures are instantly available. Pictures pass on sufficient dreary information with the objective that watermarks can be embedded easily. It may be normal that any compelling picture watermarking estimation may be upgraded for the video in addition. Pictures are addressed in spatial space similarly as in repeat region. The image in the change zone is talking its repeat coefficients and in spatial space it is addressed by pixels. Basically, change space suggests the image as various repeat gatherings.

To address an image in the change region, variable changes like Discrete Cosine Change (DCT), Discrete Wavelet Change (DWT) or Discrete Fourier Change (DFT) can be used. These progressions have its own features and address the image in its own particular habits. Watermarks can be constrained inside pictures by changing the change space repeat coefficients. An event of the spatial space; essential watermarks could be constrained in the photos by changing the pixel regards or the Least Huge Piece (LSB) values. Regardless, progressively solid watermarks could be constrained in the change space of pictures by changing repeat coefficients.

Progressed watermarking frameworks are assembled into different sorts. This request relies upon a
couple of criteria which are: Watermark Type (commotion, picture); Strength (sensitive, semi-fragile, and incredible); Space (spatial, repeat); Perceptivity (recognizable watermarking, indistinct watermarking); Host Information (picture, substance, sound, and video); Information Extraction (trance, semi-stupor, and non-stun). Necessities for picture watermarking contain vagary, life to fundamental banner getting ready assignments, and limit. Basic banner taking care of exercises which the watermark should persevere through fuse pressure, isolating, rescaling, cutting, A/D and D/A change, geometric twists, and included substance uproar.

2. LITERATURE REVIEW

A robust authentication mechanism supported linguistics segmentation, chaotic encoding and knowledge activity. Assumptive that user X needs to be remotely authenticated; ab initio X’s video object (VO) is mechanically divided, employing a head and body detector. Next, one in every of X’s biometric signals is encrypted by a chaotic cipher. Later the encrypted signal is inserted to the foremost vital ripple coefficients of the VO, exploitation it’s Qualified Significant Wavelet Trees (QSWTs). QSWTs offer each physical property and vital resistance against loss transmission and compression, conditions that are typical in wireless networks. Finally, the Inverse Discrete Wavelet Transform (IDWT) is applied to produce the stego-object (SO) [1].

Here, brand is taken into account because the watermark. the brand ought to be embedded into the first input image to create the watermarked image exploitation DWT rule and therefore the watermark (logo) was decrypted exploitation IDWT. Therefore, Digital Image watermarking is completed [2].

A completely unique image sweetening technique, named CLAHE-discrete wavelet transform (DWT), which mixes the CLAHE with DWT. The new technique includes 3 main steps: initial, the first image is rotten into low-frequency and high-frequency elements by DWT. Then, the authors enhance the low-frequency coefficients exploitation CLAHE and keep the high-frequency coefficients unchanged to limit noise sweetening. This is often as a result of the high-frequency part corresponds to the detail info and contains most noises of original image. Finally, reconstruct the image by taking inverse DWT of the new coefficients [3].

A completely unique theme of pressing encrypted pictures with auxiliary info. The content owner encrypts the first uncompressed pictures and additionally generates some auxiliary info, which is able to be used for knowledge compression and image reconstruction. At receiver facet, the principal image content are often reconstructed exploitation the compressed encrypted knowledge and therefore the secret key [4].

A robust digital watermarking theme for copyright protection of digital pictures supported subsampling. The watermark could be a binary image, which is embedded in separate remodel constant of the host image and not employed in the first image. During this theme, they’d used chaotic map in watermarked image. But the results of watermark image are sweet and strong to attack [5].

DCT primarily based watermarking theme that provides higher resistance to image process attacks like JPEG compression, noise, rotation, translation etc. during this approach, the watermark is embedded within the middle band of the DCT blocks carrying low frequency elements and therefore the high frequency sub band elements stay unused. Watermark is inserted by adjusting the DCT coefficients of the image and by exploitation the personal key. Watermark will then be extracted exploitation an equivalent personal key while not resorting to the first image [6].

A watermarking theme supported the discrete wavelet transform (DWT). The watermark, shapely as Gaussian noise, was supplementary to the center and high frequency bands of the image. The coding method concerned taking the DWT of a probably marked image. Sections of the watermark were
extracted and correlative with sections of the first watermark. If the cross-correlation was on top of a threshold, then the watermark was detected. Otherwise, the image was rotten into finer and finer bands till the whole, extracted watermark was correlative with the whole, original watermark. The matter with the projected technique is that this system is liable to geometric attacks [7].

A semi-blind reference watermarking theme supported discrete wavelet transform (DWT) and singular worth decomposition (SVD) for copyright protection and credibility. Their watermark was a grey scale brand image. For watermark embedding, their rule reworked the first image into ripple domain and a reference sub-image is created exploitation directive distinction and ripple coefficients. Then, their rule embedded the watermark into reference image by modifying the singular values of reference image exploitation the singular values of the watermark [8].

Developed AN improved wavelet-based watermarking through pixel-wise masking. It’s supported masking watermark in step with characteristics of HVS. The watermark is adaptively supplementary to the most important detail bands. The watermark deliberation perform is calculated as a straightforward product of knowledge extracted from HVS model. The watermark is detected by correlation. The projected technique is strong to varied attacks however this technique is complicated than alternative remodel technique [9].

The watermark is scaled by a saliency issue, computed on a block by block basis, counting on native image noise sensitivity. It's then repeatedly supplementary to the sub bands of DWT decomposition of host image. Visual masking is therefore exploited up to solely block resolution. A code is embedded by appropriately quantizing the coefficients of detail bands. For watermark recovery, the embedded code is calculable by analyzing coefficients quantization. Once the code is calculable, it's correlative and results compared to a threshold chosen on the premise of a given false positive likelihood [10]. Various operators were used for digital watermarking system [11].

This article was given the overview of current attacking methods, statistical analysis of the original data and the embedded watermark and stochastic formulation of estimation-based attacks for watermarking [12].

3. OBJECTIVES

- Digital watermarking is now an importantly focused technique aimed at providing a reliable way to protect images or authenticate copyrights protection.
- In the existing mode such as spatial domain, the watermark is not properly embedded and extracted and it leads to improper protection of secret information.
- The existing spatial domain is transformed into frequency domain using discrete wavelet transform.
- In our proposed work the watermark is usually embedded invisibly in the images to avoid attracting the attention of malicious attackers. We are using color image watermarking, which has high efficiency compared to the traditional gray scale image watermarking.

4. PROPOSED SYSTEM

Figure 1 shows that the block diagram for proposed watermarking system. Proposes a confused encryption based outwardly disabled propelled picture watermarking technique fitting to both dim scale and concealing pictures. The watermark introducing unit and watermark security unit structure two basic sub-systems of the proposed system. The watermark security unit is away for improving the shield of the introduced watermark so as to make it unlimited for an adversary to get the cautious watermark paying little mind to whether it has the data of embedding count. Tempestuous speculation and Arnold encryption are used to achieve a predominant security. The numerical ground works of
Bedlam and Arnold encryption are shown in the going with sub section.

4.1 **Discrete cosine transform**
Discrete cosine change (DCT) is comprehensively used in picture getting ready, especially for pressure. A part of the usages of two-dimensional DCT incorporate still picture weight and weight of individual video traces, while multi-dimensional DCT is the part utilized for pressure of video streams. DCT is likewise helpful for exchanging multidimensional information to recurrence area, where distinctive activities, similar to spread range, information pressure, information watermarking, can be performed in less demanding and progressively productive way.

4.2 **Arnold and Chaotic**
Arnold transform is the effective technique for safeguard of information which is increased by using enormous encryption techniques. This inscription method is two dimensional. It will be used for in creation images of type N×N.

The consequence of Arnold change is an encoded picture which has a balanced correspondence with the first picture. A chaotic based encryption algorithm is an active method for image encryption.

4.3 **Methodologies**

4.3.1 **Image Encryption.**
The authentic image is in an encompassed pattern and that the pixel values are within [0, 255], and intend the numbers of rows and columns as N₁ and N₂ and the pixel number as (N=N₁ X N₂). The watermark is embedded into the original input image.

A chaotic based encryption calculation is a functioning technique for information encryption.

Arnold transform is an encoded picture which has a balanced correspondence with the first picture.

4.3.2 **Encrypted Image Encoding.**
The secret data was entered in text format into the watermarked image. If the keyword was matched, then only it moves to the next step. i.e., reconstruction, otherwise if the keyword does not match it results in the error.

4.3.3 **Image Watermark Extraction.**
With the watermark embedded image and the secret key (keyword), a receiver can regenerate the primary information of the original image, and the resolution of the reconstructed image is dependent on the number of level of watermark.

![Figure 1. Block Diagram for Proposed watermarking system](image-url)
4.4 Algorithm Used
RGB to Channel Conversion
Once the images are resized the image is split into three individual colors as Red, Green and Blue.
Algorithm:
Step 1: Read an original image by specifying the file name and image format such as jpg etc
   \[ \text{Img} = \text{imread}('\text{filename.png}') \]; % Read image
Step 2: Specify individual color name as shown
   \[ \text{Red} = \text{img}(:, :, 1); \] % for red channel
   \[ \text{Green} = \text{img}(:, :, 2); \] % for Green channel
   \[ \text{Blue} = \text{img}(:, :, 3); \] % for Blue channel
Step 3: Display the images using imshow function.

5. RESULT ANALYSIS

![Figure 2](image1.png)

**Figure 2.** Original Image going to watermark and Watermarked Image in Matlab

The original image (figure 2) is resized to a standardized size since size of different images varies.
After Resizing image will be transformed as of RGB towards gray scale image evaluated by way of
Channel separation. Figure 3 shows discrete wavelet transform output of given input image from
default images of mat lab software.

![Figure 3](image2.png)

**Figure 3.** Results for watermark embedding
Figure 4 shows the process of key entering to retrieve the watermarking image through MATLAB software.

Figure 5 shows the process of key entering to retrieve the watermarking image through MATLAB software. After entering wrong key, it shows keywords not matched.

The analysis is done for 4 to 6 images which are present default in MATLAB. Performance measure such as PSNR, MSE is determined. Results were satisfactory compared to existing method. The performance parameters of the proposed system are evaluated as shown in Table 1 and Figure 6.

| Proposed method | PSNR  | MSE   |
|------------------|-------|-------|
|                  | 74.6862 | 0.0022 |
6. CONCLUSION

A secure and blind watermarking scheme in the DCT domain was used with recent methods. Arnold transform and chaotic encryption were utilized to tote double coat safeguard to the watermark. The double layer of security of the implanted watermark guarantees that the plan is profoundly secure in nature. We presume that it is appropriate for the use of copyright insurance and proprietorship verification.

REFERENCES

[1] Klimis Ntalianis, and Nicolas Tsapatsoulis 2015 IEEE Trans EMERG Top Com 4 156
[2] Mehran Andalibi, and Damon M 2015 IEEE Trans Image process 24 5060
[3] Huang Lidong, Zhao Wei, Wang Jun, and Sun Zebin 2015 IET Image processing 9 908
[4] Xinpeng Zhang, Yanli Ren, Liquan Shen, Zhenxing Qian, and Guorui Feng 2014 IEEE Trans Image process 16 1327
[5] W. Hong, and M. Hang 2006 IEEE Trans. Signal Process 12 1
[6] Blossom Kaur, Amandeep Kaur, and Jasdeep Singh 2011 IJAET 1 72
[7] X. Xia, C. Boncelet, and G. Arce 1997 IEEE Int. Conf. on Image Processing 7 548
[8] Bhatnagar, G. and Raman, B 2008 Comput Stand Inter 31 1002
[9] Barni M, Bartolini F, and Piva 2001 IEEE Trans image process 10 783
[10] D. Kundur and D. Hatzinakos 1998 IEEE ICASSP 6 2969
[11] H. Tao, L. Chongmin, J. M, Zain, and A. N. Abdalla 2014 JART 12 122
[12] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su 2001 IEEE Commun. Mag 39 118