Enhanced Techniques using Dual watermarking for DWT, DCT and SVD

D.S. Somra¹, M. Gupta²

¹,²Dept. of CSE, VITM, Gwalior, India

*Corresponding Author: deepak.somra789@gmail.com, Tel.: +91-8085527654

DOI: https://doi.org/10.26438/ijcse/v7i2.190197 | Available online at: www.ijcseonline.org

Abstract—Digital image watermarking (DIW) is the way toward embedding watermark into a digital image (DI) for validation and in this way protecting the DI from copyright encroachment. In this paper, a versatile undetectable watermarking plan is paper in dual watermarking process. It is expected that the simplicity with which advanced media can be replicated will prompt an expansion of copyright encroachment. The implement work calculation is depicted in subtle elements. The 2 transform and dual watermarking are useful in course in such an approach to misuse their appealing properties. In this method, the wavelet coefficients of the cover image to embed the watermark. The four sub bands of wavelet coefficients can be used to watermark the image. The new DCT coefficients form the singular value decompositions triangular matrices. Then the inverse DCT transform is applied by the inverse DWT. Watermark embedded using this algorithm is highly imperceptible. This scheme is robust against all sorts of attacks. It has very high data hiding capacity.

Keywords—Digital image Watermarking, Dual watermarking, Image processing, DWT; DCT; SVD.

I. INTRODUCTION

With the multimedia information processing technology and the rapid development of computer networks, people get through the network more media and increasingly more and more convenient. Digital images are the most common kind of multimedia information, and it has become our main way to get and publish information. However, the large numbers of digital image processing software (such as Photoshop) continue to improve the function. So people can easily perform edition, production and other operations on these images, which greatly facilitates the user. Meanwhile the integrity of the image information, the authenticity of the content and other security problems eleven exposed. Therefore, the authentication of the digital image and the integrity protection has become to be solving the problem. [1].

Digital watermarking (DW) is the strategy in which an visible/invisible signal (watermark) is implanted in an interactive media archive for copyright protection (CP). It is a mix of a noticeable watermark and an imperceptible watermark picture and to distinguish minute alteration of a picture and to insert the watermark mid recurrence band of a second level DWT change was utilized. This becomes particularly important as the technological disparity between individuals and organizations grows. Governments and businesses typically have access to more powerful systems and better encryption algorithms than individuals. Hence, the chance of individual’s messages being broken increases which each passing year. Reducing the number of messages intercepted by the organizations as suspect will certainly help to improve privacy. [2]

Digital Watermarking Fundamentally watermarking can be defined as “the process of engrafting a watermark in a multimedia object”. The watermark technique divulges the ownership of the multimedia object. The basic rationalities of embedding watermark are copyright protection, content authentication, temper detection etc. visible and invisible watermarks can be embedded in the multimedia object. Requirements of Digital watermarking have three main requirements. They are transparency, robustness and capacity.

A. Transparency or Fidelity Transparency explicates that the quality of the image is not compromised after the watermark is applied on it. Cox et al. (2002) define transparency or fidelity as “perceptual similarity between the original and the watermarked versions of the cover work”. Transparency ascertains that there should not be any visible distortions in the image after watermarking is applied to it because it scales down the commercial value of the image.

B. Robustness Cox et al. (2002) defines robustness as “ability to detect the watermark after common signal processing operations”. A watermarked image is intentionally and unintentionally removed by a simple image processing like contrast or brightness enhancement (unintentionally) and compression, compression, filtering (intentionally). Stirmark, a benchmark to test robustness of watermarking algorithm, categorizes the attacks as
1. Attack that bump off the synchronization between embedded and the detector.
2. Attack that try to remove watermark totally.
3. Cryptographic attacks
4. Protocol attacks

C. Capacity or Data payload “The number of bits a watermark encodes within a unit of time or work” defines the capacity or data payload cox et al. (2002). This property manages the amount of data that should embed as a watermark for successful detection during extraction. Watermark should contain optimal information to represent the uniqueness of the image. Watermarks and Watermark Detection The main types of watermark that can be embedded within an image: -

A. Pseudo – Random Gaussian Sequence

A Gaussian sequence watermark is a chronological sequence of numbers comprising 1 and -1 which contains comparator 1’s and -1’s. This sequence is represented as a watermark with zero or one variation. A correlation measurement is used for the object detection in watermarking.

B. Binary Image or Grey Scale Image Watermark

This approach uses a logo image rather than a pseudorandom Gaussian sequence to embed substantive data by employing various watermarking techniques. For the spotting of the watermark, a set aside decoder has to be designed based on the type of watermark embedded. A hypothetical testing is to be exercised for the detection of the presence of watermark in a Pseudo-Random Gaussian Sequence. W is the original and W’ is the extracted, watermark bit sequence respectively. BER (Bit Error Rate) is calculated to detect the presence of watermark. Zero value of BER, show the presence of watermark and if BER is one then there is no watermark.

In Binary Image Watermarking, Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two metric functions used to compare the original image and the watermarked image in Binary Image Watermarking. It uses standard criteria as[3]

\[
MSE = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (I(x,y) - I'(x,y))^2 / M \times N
\]

And

\[
PSNR = 20 \times \log_{10} \frac{255}{\sqrt[2]{MSE}}
\]

1.2 OBJECTIVE:

A Dual watermarking method using multiple watermarks is a software application that enhances the security level, which embeds both visible and invisible several watermarks. This application can access online and authorized user can add multiple watermarks to image for security. The systems target is when pirated picture is found, users can extract the watermark from picture to prove the identity of the original user. The objective for the advancement of the proposed framework is to check the attainability of invisible watermark and VW and concentrate the impedance of watermarks with one another and furthermore to lessen this obstruction at various phases of watermarking. At the point when the responsibility for unmistakably WI is being referred to, the undetectable watermark can be extricated to give proper proprietorship data. Important points about an application: [4]

- It will be very easy for the user of this application to provide security to own images.
- Easy to add watermarks, Extraction and prove the user identification.
- Watermarks are not affect original quality of the image.

II. DUAL WATERMARKING

In this paper, a DI double watermarking plan is displayed. In the plan, robust watermark (RW) is incorporated with fragile watermark (FW). RW is the copyright image of DI and FW is an approving validness estimation to affirm the alter status of DI. Both of two watermarks are implanted in spatial space. Twofold keys, installing and correlative recouping methods for non-plane and a few characters in view of HVS property are presented amid implanting RW, while FW, receiving spatial space low piece plane arbitrary inserting route went for pixels. The plan is a successful estimation to decide the validness and integrality of a picture.

2.1 Dual watermarking technique

It is a blend of a VW with an undetectable watermark. At the point when the responsibility for WI is being referred to, the imperceptible watermark can be removed to give suitable possession data. There is not really any exploration work completed utilizing double watermarking system. Mohanty et al (1999) exhibited a double watermarking method which endeavors to build up the proprietor's entitlement to the picture and distinguish the deliberate and unexpected altering of the picture. Be that as it may, this near the beginning investigate is just a blend of obvious and IW calculations. It originally utilized a square DCT founded obvious watermarking calculation to insert a dim scale WI, and after that considered the subsequent picture as another picture to do IW. Invisible watermarking (IW) is presented in SD. They stated so as to if everyone endeavors to alter the VW purposely, they can make out the level of hardening with the assist of undetectable watermark acknowledgment count. Hu

Watermark A

Watermark B

Host Image I

Watemarked image I' A

Watemarked image I' B

1st Stage          2nd Stage

Fig. 1. Dual watermark scenario

3.3. Watermarking Perception

In light of human observation, DW can be isolated into visible and invisible perception.

Visible Watermark (VW): In VW the watermark shows up, data is noticeable to a watcher in video or picture just on cautious examination [6]. For instance a TV stations, as BBC, whose logo is obviously superimposed at the intersection of TV.

Invisible Watermark: The invisible watermark is completely imperceptible. The invisible-RW is installed so that modifications made to the pixel esteem are perceptually not detectable and can be recouped just with the suitable translating system. The undetectable FW is implanted so that any control or adjustment of the picture would modify or crush the watermark. Invisible watermark can be further divided into three types:

1) Robust Watermark: It aims to embed information in a file that cannot be easily destroyed. They are designed to resist any manipulations that may be encountered. All applications where security is the main issue use robust watermarks.

2) Fragile Watermark: They are designed with very low robustness. They are used to check the integrity of objects.

3) Public and Private Watermark: They are differentiated in accordance with the secrecy requirements for the key used to embed and retrieve watermarks. If the original image is not known during the detection process then it is called a public or a blind watermark and if the original image is known it is called a non blind watermark or a private watermark.

Dual Watermark: It is a mix of an unmistakable and an undetectable watermark [6]. Their work first embeds the visual watermark in the first picture and after that an undetectable watermark is added to the officially visual WI. The last WI is the dual watermarked picture.

2.4. Watermarking Domains

Watermarks can be embedded either in the spatial or the change space as talked about underneath.

Spatial Domain (SD): The SD systems straightforwardly adjust the power estimations of some chose pixels. SD likelihood depend watermarking plan for shading pictures is proposed in. Their strategy ended up being vigorous to different IP activities.

Transform Domain (TD): The watermarking method depends on the TD can be additional ordered into the DFT, DCT and DWT area strategies.

DFT: The DFT changes over a restricted once-over of likewise isolated models of a limit into the once-over of coefficients of a constrained mix of complex sinusoids, asked for by their frequencies, that has those same example esteems. Introduced a calculation for pivot and scale invariant watermarking of DW. Their exploratory outcomes are powerful to pressure, sifting, trimming, interpretation and revolution.

DCT: A DCT conveys a constrained course of action of data centers the extent that a total of cosine limits influencing at different frequencies. A spread-range like DCT domain watermarking procedure for CP of still advanced pictures is investigated in. The DCT is connected in squares of 8 x 8 pixels as in the JPEG calculation.

DWT: The WT depends on little waves. The heart of wavelet analysis is multi resolution analysis. In 2D DWT, every one level of rot create 4 gatherings of info, single contrasting with the low low band (LL), and 3 additional identifying with horizontal (HL), vertical (LH), and diagonal (HH) sub-groups. A DWT based IW. Considered watermarking constructed plot in light of Least Significant Bit (LSB) and the DCT under spatial and recurrence space. Their exploratory outcomes exhibited the enhanced execution of the DCT as far as impalpability and heartiness when contrasted with the LSB space.

III. USING TECHNIQUES

In this paper using techniques:

A. Discrete Wavelet Transform (DWT)

DWT is a method for analyzing multi-level signal it can analyze the signal at different frequency bands with different resolutions by decomposing it into approximation and detailed information. The principle of the algorithm is to divide the image into four at each iteration, three blocks on the details of the image (LH, HL, HH), and the fourth (LL) corresponds to the most important information for the eye (low frequencies), which serves basis for the next iteration. To decompose this image into sub image we use: high and low pass filters (LPF). The DWT can be expressed as follows:

$$\psi_\alpha(t) = \int f(t) \frac{1}{\sqrt{a}} \psi_\alpha \left( \frac{t - b}{a} \right) dt$$
B. SVD based watermarking

It is a numerical analysis device used to diagonalize matrices. It is advanced for a selection of packages algorithm. The most important properties of the SVD in terms of image processing (IP) applications are: Singular values (SVs) of the picture have very good balance to understand while a small perturbation is made inside the picture of the SV does not alterate extensively; SV is an algebraic intrinsic belongings. SVD processing in a matrix A can be decomposed into three matrices of the equal size because the preliminary matrix; two orthogonal matrices U and V and a diagonal matrix S.

\[ A = U \times S \times V^T \]

The columns of U and V are called respectively left and right singular vectors of A. They essentially determine the details geometry of the original image. The diagonal values of the matrix S are ranked in descending order. \[ \sigma_1 \geq \sigma_2 \geq \sigma_3 \geq ... \geq \sigma_R \geq \sigma_R + 1 \geq ... \geq \sigma_N = 0 \]

C. Discrete cosine transforms (DCT)

First of all image is segmented into non overlapping blocks of 8x8. Then every of those blocks ahead DCT is implemented. After that some block selection criteria is applied and then coefficient selection criteria is applied. Then watermark is embedded by using modifying the chosen coefficients and ultimately on every 8x8 block inverse DCT remodel is applied.

\[ y(j, k) = \frac{2}{M} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} x(m, n) \times \cos \left( \frac{(2m + 1)\pi}{2M} \right) \cos \left( \frac{(2n + 1)\pi}{2N} \right) \]

\[ a_j = \sqrt{\frac{2}{N}} \text{ if } j = 0 \text{ or } j = 1, 2, ..., N - 1 \]

\[ a_k = \sqrt{\frac{2}{M}} \text{ if } k = 0 \text{ or } k = 1, 2, ..., N - 1 \]

IV. LITERATURE SURVEY

Zigang Chen, et al. (2018) [8] In this paper, we analysis a new General-NMF (General non-negative lattice factorization) founded DW conspire for duplicate insurance and respectability verification of the picture content. Moreover, the producer issue of the irregular framework and n are utilized as the keys of the analysis DW plan. New outcomes about demonstrate that the proposed DW plan can successfully oppose different attacks and altering.

Ninny Mittal, et.al. (2017) [9] In this test, we projected optical watermarking (OW) for using pictures which relies upon the mix of 5 DWT, FFT and SVD. Another point of view of this examination is to discover the life of the VW plan, which is emerge of progression that can incorporate watermarked information to address picture data carried with front line cameras with no particular additional equipment's fundamental building..

Alifa D’Silva, et al. (2017) [10] In this paper a hybrid method utilizing SVD and DWT is individual planned. SVD and DWT are network depend tasks, crossover technique forestalls difficulty which would somehow expend a great deal of assets. Calculation of a bigger arrangement of information happens quicker because of the utilization of SVD. This plan has been recreated in MATLAB condition.

Guang Hua, et al. (2016) This paper analyzes such a dual channel scheme from the perspective of digital filtering. We show that the dual channel based watermark extraction actually applies a high pass filter to the watermarked signal, and the performance when the filter coefficients are changed is also studied. The effectiveness of the dual channel scheme in rejecting host signal interference is confirmed via extensive experiments using both synthetic and real audio and image signals.[11]

Jin-Xia Yang, et al. (2017) In order to improve the security of dual watermark, a novel dual audio watermarking scheme based on wavelet packet analysis and ultra-chaotic encryption is proposed. First, accuracy parameters are selected to generate super chaotic sequence and ultra-chaotic binary sequence which are used to encrypt zero-watermark sequence and image watermark acquiring more evenly distribution. Finally, simulation platform is utilized to test the performance of the algorithm.[12]

Qing Chen, et al. (2016) This paper proposes an algorithm of dual watermarking based on wavelet transform for data protection in smart grid. Two different watermarks, robustness watermark and fragile watermark, are embedded in the significant coefficients of DWT to protect both copyright and integrity of data. [13]

Jeebananda Panda, et al. (2016) Digital watermarking is a technique to employ copyright protection and ensure the authenticity of the owner using a proof of ownership embedded in a multimedia file. The watermarked video is subjected to different attacks and the efficiency of the technique is measured using Correlation Factor and PSNR. The algorithm presented is robust, secure and is energy efficient with decreased payload on the host signal.[14]

Sawiya Kiatpapan, et al. (2015) This paper describes an image tamper detection and recovery method based on self-embedding dual watermarking. This dual watermarking strategy ensures a robust performance in image tamper detection and recovery. This makes it possible to recover large area of tampering, such as, left, right, upper, or lower half of the cover image.[15]
Jingchun Zhang, et al. (2011) This paper presents a dual watermarking scheme of digital images based on the dynamic feature points. In our dynamic feature watermarking scheme, the watermarking energy distributes on the dynamic feature set extracted by the key-decided orthogonal vector operator and a dual watermark that is formed embedding copyright watermark into another child watermark consisting of features selected from the digital images is embedded into the circumjacent area of feature points through Chaotic sequence.[16]

Daojing Li, et al. (2010) In this paper, we proposed a Dual Watermarking Scheme Based on Threshold Cryptography (DWTC) for Web Document to resolve the two problems. DWTC consists of watermark generation, embedding and detection process. Based on threshold cryptography, watermark generation process can enhance the robustness. To recover the embedded watermark only parts of watermark slices are needed. Experimental results show that the DWTC effectively achieve both the invisibility and robustness.[17]

V. PROPOSE WORK

Problem statement
In this method the wavelet coefficients of the cover image to embed the watermark. The four sub bands of wavelet coefficients can be used to watermark the image. The DCT coefficients of the wavelet coefficients are calculated and singular values decomposed. The same procedure is applied to the watermark also. The singular values of the cover image and watermark are added to form the modified singular values of the watermarked image. The new DCT coefficients form the singular value decompositions triangular matrices. Then the inverse DCT transform is applied by the inverse DWT. This is the algorithm that clubs the properties of SVD, DCT and DWT. This is a technique that has never been used before. Watermark embedded using this algorithm is highly imperceptible. This scheme is robust against all sorts of attacks. It has very high data hiding capacity.

Propose Algorithm:
1. First we browse cover image from dataset.
2. Then we browse watermark image from dataset.
3. Apply DWT, DCT and SVD to watermark image.
4. Apply DWT to again watermark.
5. Then extract watermark image.
6. Again extract watermark image by DWT, DCT and SVD.
7. Calculate the parameter PSNR value for extracted image.
8. Exit.

VI. RESULT ANALYSIS

Fig. 2. Propose methodology

Fig. 3. First, We ‘Run’ our code and then obtain this type of menu bar. In this menu bar there are 8 steps.
Fig. 4. first we browse cover image from dataset.

Fig. 5. we browse watermark image from dataset.

Fig. 6. watermark with DWT DCT and SVD

Fig. 7. dual watermark with DWT

Fig. 8 extract watermark image

Fig. 9. extract dual watermark image

Table 1. Comparison on Base PSNR and Propose PSNR

<table>
<thead>
<tr>
<th>Image Name</th>
<th>Base PSNR</th>
<th>Propose PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image 1</td>
<td>36.2089</td>
<td>42.7501</td>
</tr>
<tr>
<td>Image 2</td>
<td>36.1321</td>
<td>66.1818</td>
</tr>
</tbody>
</table>
VII. CONCLUSION AND FUTURE SCOPE

Dual Watermarking is the better process of hiding some data or information in an appropriate multimedia file as for example image, audio and video files. It comes under the evidence that if the feature is visible, the chances of attack is evident, thus the goal of invisible watermarking is always to conceal the very existence of the embedded data. It has been propelled to the forefront of current security techniques by the remarkable growth in available digital media via World Wide Web. Dual Watermarking technology plays an important role in securing business as it allows placing an imperceptible mark in the multimedia data to identify the legitimate owner.

This paper implemented DCT 3DWT-SVD scheme has proved a high degree of robustness against majority of attacks including noise, blurring, other kinds of image processing attacks which can be validated by recovering the watermark from any of the sub-band, which clearly indicates that transform domain is more robust than spatial domain Method. Calculate the PSNR value for extracted image.

REFERENCES


[5] VANDANA S INAMDAR1,∗ and PRITI P REGE2, “Dual watermarking technique with multiple biometric watermarks”.

Graph. 1. Comparison on Base PSNR and Propose PSNR

<table>
<thead>
<tr>
<th>Image Name</th>
<th>Base MSE</th>
<th>Propose MSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image 1</td>
<td>0.1342</td>
<td>0.1226</td>
</tr>
<tr>
<td>Image 2</td>
<td>0.1348</td>
<td>0.1251</td>
</tr>
</tbody>
</table>

Graph. 2. Comparison on Base MSE and Propose MSE

<table>
<thead>
<tr>
<th>Image Name</th>
<th>Base SSIM</th>
<th>Propose SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image 1</td>
<td>0.1916</td>
<td>0.9838</td>
</tr>
<tr>
<td>Image 2</td>
<td>1.7998</td>
<td>1.0000</td>
</tr>
</tbody>
</table>

Graph. 3. Comparison on Base SSIM and Propose SSIM

<table>
<thead>
<tr>
<th>Image Name</th>
<th>Base Entropy</th>
<th>Propose Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image 1</td>
<td>3.3751</td>
<td>7.3403</td>
</tr>
<tr>
<td>Image 2</td>
<td>0.9895</td>
<td>7.5102</td>
</tr>
</tbody>
</table>

Graph. 4. Comparison on Base Entropy and Propose Entropy
S. Sadhan Vol. 39, Part 1, February 2014, pp. 3–26. c Indian Academy of Sciences


[8] Zigang Chen, Lixiang Li, Haipeng Peng, Yuhong Liu, and Yixian Yang, “A Novel Digital Watermarking based on General Non-negative Matrix Factorization”. This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2018.2794985, IEEE Transactions on Multimedia


