A CRT BASED ROBUST IMAGE WATERMARKING USING DISCRETE TCHEBICHEF TRANSFORM

J. L. Divya Shivani and Ranjan K. Senapati
Department of Electronics and Communication, K. L. University, A. P., India
E-Mail: shivandivy18@gmail.com

ABSTRACT
This paper presents a Chinese Remainder Theorem (CRT) based digital watermarking technique in Discrete T-Chebycheff Transform (DTT) domain which is robust to several common attacks. The proposed technique is compared with the recently proposed CRT based Discrete Cosine Transform (DCT) domain technique. Extensive simulation experiments show the better robustness to the common image manipulations such as brightening, sharpening, cropping, noise and compression. At the same time, the proposed technique successfully makes the watermark perceptually invisible. Better Tamper Assessment Function (TAF) value of 30-40% is achieved in comparison to 30-40% in DCT and 10-40% on Singular Value Decomposition (SVD) techniques. Similar to DCT domain watermarking, it is possible to maintain the imperceptibility and low TAF for various values by doubling the capacity of the watermark.

Keywords: Chinese remainder theorem, discrete cosine transform, discrete tchebichef transform, imperceptibility, tamper assessment factor.

1. INTRODUCTION
With the rapid growth in technology and internet applications it made easy access for every user to download multimedia data like images, videos etc. through the internet, whereas this data can easily be tampered or manipulated, for which data integrity must be ensured. Digital watermarking is used to verify integrity. There are many techniques in watermarking owing to the characteristics, imperceptibility, inseparability from the cover content and its inherent ability to undergo the same transformations as experienced by the cover content. Among the techniques, this is efficient only if the watermark is imperceptible, secure and robust.

Digital watermarking techniques are performed in the spatial domain [1] [2] and in transform domain [1] [3]. Transformed domain is more robust and provides more imperceptibility than spatial domain [5]. In transform domain DCT make use of energy distribution properties and human visual system scheme for embedding watermark. Blind watermarking scheme [5] [6] with interesting results have been proposed. Some of the other transformed-domain watermarking schemes have been proposed in SVD and also used in watermarking (where the properties of U coefficients [10] [12] modification cause less degradation of image quality. Some of the watermarking techniques using Ridgelet transform also proposed.

CRT based scheme which provides robustness against some common image processing manipulations are proposed. Digital watermarking is also performed using segmentation of DCT blocks. Each DC coefficients is extracted and stored in a matrix before processing making it expensive in terms of memory requirement, techniques were developed to use middle DCT coefficient for embedding watermark. The algorithm is not much robust against JPEG compression. Watermarking schemes can be implemented in VLSI chips. Hardware implementation in consumer electronic devices such as digital camera, PDAs, and mobile devices requires low power, high reliability, real-time performance and easy integration. For example, viability of integration of watermarking chips in any digital camera/JPEG codec. Several issues related to hardware implementation of several watermarking algorithms for images and videos [8] [9].

DCT domain watermarking is popular for hardware implementation because there are a number of fast algorithms [5] [6]. 8x8 DCT is mostly used for hardware implementation. 4x4 DCT provides less computation at a cost of less energy compaction.

Discrete Tchebichef Transform (DTT) is a new transform and has relatively similar properties with DCT. The properties include (i) Energy compaction, (ii) Seperability and Symmetry, and (iii) Orthogonal. There are many works related to compression. DTT can be used in applications such as feature extraction, pattern recognition, blind integrity verification, and artifact measurement. However, to the best of our knowledge no such work in Security applications have been reported in the literature. This paper presents a novel robust image watermarking scheme in DTT domain. The scheme uses CRT for its robustness. As the polynomials of DTT matches closely with HVS, the scheme provides higher perceptual quality than DCT based watermarking scheme. The proposed methodexhibit superiority in terms of SSIM and TAF over most of the schemes. Good TAF values are also obtained in case of most of the common attacks such as cropping, tampering, noise addition, brightening, sharpening and compression. Attacks such as scaling, rotation, filtering and geometric transformation are not considered in this paper.

The rest of the paper is as follows: Section 2 discusses the implementation of embedding and extraction aspect of the proposed scheme. Comparison results are presented in Section 3. Finally, in Section 4 conclusion and future research direction have been made.

3600
2. PROPOSED SCHEME
The block diagram of the proposed scheme is shown in Figure-1. The uniqueness of the scheme is that the ‘key’ is generated randomly during embedding process instead of using a known key for embedding compared to other methods. Along with watermarked image, the key will be send to the receiver.

The embedding and extraction technique of the proposed method is based on the combining CRT technique in the DTT domain. This method produces the better security, the better robustness and also needs the simple operation during extraction phase.

2.1 Embedding procedure
The following steps describe the watermark embedding procedure on the host image.

Step-1. Partition of blocks
The host image is taken as a gray scale image and watermark is a binary image. Initially, the host image is divided into blocks of 8 x8 pixels. The single watermark bit is then embedded in a single block selected. Then the blocks are chosen as random.

Step-2. Selection of DTT coefficients
In order to improve robustness, the preferred choice is to embed the watermark into the most significant coefficients. However, it will degrade the quality of the watermark. If insignificant coefficients are used for embedding, the watermark may have lost during lossy compression [8] [9]. Since proposed scheme use block size 8x8 pixels, resulting DTT block is also of same size. This gives a total of 64 DTT coefficients.

Step-3. Randomization
After zig-zagging the DTT coefficients, one value must be selected. During that selection randomizing the coefficients is done using Arnold Transform instead of using the regular selection procedure. Using randomization technique, security and authentication are more as the value is changing for every execution. During randomization, one of the selected coefficients is chosen and it is stored as a secret key whenever we execute the code. This feature adds more security to the data while embedding and extraction procedure.

Step-4. Embedding the watermark bits
After dividing 8x8 blocks, one watermark bit gets embedded in each of the block. Considering one block at a time, the procedure for embedding the watermark bits is listed as follows:

a) Randomly select 8x8 block from host image and apply DTT to the block.

b) Randomly select a watermark bit from the watermark image in order to embed into the block.

c) Randomly select a DTT coefficient (DC or one of the AC components) to embed the watermark bit. Let its value be denoted as $X$.
d) Let $P_1$ and $P_2$ be the pair-wise co-prime numbers used in CRT (say, $P_1=38$ and $P_2=107$) for the DC coefficient. For an AC coefficient, let the values of $P_1=38$ and $P_2=55$.

e) Find $E_1$ and $E_2$ by applying the inverse CRT to $X$.

f) Determine the values of $z'$ and $X'$.

g) The required condition for embedding watermark bit '1', is $z \geq X/u$ (1) where $u=2$ if X is DC coefficient, otherwise, $u=4$. If condition is not satisfied, then $X$ is modified to $\hat{X}$ until the required condition in (1) is satisfied.

h) The required condition for embedding watermark bit '0' is $z < X/u$ (2). If the condition in (2) is not satisfied, then $X$ is modified to $\hat{X}$ until the required condition is satisfied. The process of the embedding bit '0' and the bit '1' is illustrated in the Flow Chart Figure-2.

i) Reconstruct DTT block with the modified DTT coefficient, $\hat{X}$ and apply inverse DTT to the block to construct the watermarked image block.

j) Repeat the steps 1-9 for all the remaining blocks until all the watermark bits got embedded.

Note that the range of possible values for DC and the AC coefficients are not the same. The range of the DC coefficient is from values 0 to 2040 and for AC coefficients, it will be from -1020 to +1020 in monochrome images. According to CRT, the product of the pair-wise co-prime numbers (also called the dynamic range) must be greater than the largest possible number (Patra et al., 2010).

The flow chart for embedding procedure is shown in Figure-2.

2.2 Extraction procedure

The procedure of extraction is that reverse of embedding procedure. Figure-3 shows the extraction process. For this, following information must be known to get watermark extracted from watermarked image: (i) Image which is watermarked, (ii) Size of watermark, (iii) Watermark Key, and (iv) A pair-wise numbers of co-prime $P_1$ and $P_2$.

With knowledge of the watermark key, the DTT coefficient that is embedded with watermark information $X$ is extracted. Thus, with values of $P_1$, $P_2$ and $X$, the $E_1$, $E_2$, $X'$, and $X$ are calculated.
E2 are determined. Next, comparison is made between the z and X. If $z = X/u$, the bit ‘1’ would be get extracted, otherwise the bit ‘0’ would be get extracted. The scale factor, u is then set to 2 for the coefficient of DC otherwise it is get set to 4. Thus the above steps were then repeated until every block consecutively to get all watermark bits extracted.

3. EXPERIMENTAL RESULTS

The performance of the proposed method with other schemes is evaluated using (i) Peak signal-to-noise ratio (PSNR), (ii) Tamper Assessment Function (TAF) and (iii) Structural similarity (SSIM).

Figure-3. Extraction of watermark.

Figure-4. Original(a) Lenna, (b) Watermark (c) Watermarked image (35.6 dB), (d) Reconstructed watermark (TAF-32%)

Table-1. Time complexity (in sec) comparison.

<table>
<thead>
<tr>
<th>Images</th>
<th>Patra et al</th>
<th>Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lenna</td>
<td>8.544</td>
<td>12.02</td>
</tr>
<tr>
<td>Mandrill</td>
<td>8.504</td>
<td>12.07</td>
</tr>
<tr>
<td>Barbara</td>
<td>8.469</td>
<td>11.96</td>
</tr>
</tbody>
</table>
Figure-5. (a)-(b) show the test image (Lenna) and watermark image. Figure-4 (c) and (d) show the watermarked image and extracted watermark, respectively. We have tested the watermarked image with various common attacks like, cropping, Noise addition, Brightening, Sharpening, Compression. The TAF comparison plots are presented in Figure-5 (a)-(e). It is observed that using the proposed technique the watermark image can be restored. From Figure-5, the proposed technique exhibit better watermark image in (b) cropping, (c) noise (d) sharpening, (e) brightening and compression operation than (Patra et al., 2010). However, the quality of the watermark is 30-40% in both schemes. As the proposed algorithm uses CRT for embedding the watermark in the host image, additional robustness is achieved at the cost of TAF value.

Figure-6. MSSIM performance of Watermarked image under without attack.
It was demonstrated that the SVD [10] [12] and CRT based spatial domain technique do not work for cropping, brighten, sharpen and compression operations. The proposed technique is better than SVD [10] [12] and CRT based, because it can withstand all aforementioned operations. Considering the case about the reconstructed watermarked image quality, our technique exhibit better visual quality than the other existing schemes [7] [21]. The improvement in SSIM value from Table-2 is a clear evidence of the reconstructed watermarked image quality. Table-4 shows the reconstructed watermark quality comparison under different attacks. It has been seen that the reconstructed image quality is robust to almost all attack.

Table-1 shows the time complexity of the watermark embedding and extracting process. It shows that the proposed technique has more time complexity (about 4 sec) than DCT based technique. This is because; DTT execution time is more than DCT. The higher order polynomials of DTT, depend on recursive relationship with lower order polynomials, it is not the case for DCT. Therefore, the iterative nature of DTT consumes slightly more time than DCT. However, this is trivial in hardware implementation as the Hardware uses DTT kernel coefficients like DCT. Therefore, the proposed method will exhibit similar time complexity as with DCT in a hardware platform. PSNR and SSIM comparison [13] [17] is between DCT and DTT watermarking scheme is shown in Table-2. Table-3 shows the TAF quality comparison between DCT and DTT schemes. It is evident that DTT based scheme outperform in most of the cases compared to DCT scheme.

4. CONCLUSION AND FUTURE SCOPE

A new approach of watermarking scheme using CRT on DTT domain for authentication and copyright protection is proposed. Incorporation of CRT gives advantages in terms of improved security and low computational complexity. In addition to the above, further security feature due to random selection of watermarking blocks and location of watermarked bits is incorporated. The performance of the proposed scheme is compared against CRT based DCT scheme for common attacks. It is shown that it performs well for some major attacks such as brightening, sharpening, cropping and compression. As the computation of CRT is modular, the time required for embedding and extraction depends on the type of transform. The proposed scheme is slightly

**Table-2. PSNR and SSIM comparison table for Lenna image.**

<table>
<thead>
<tr>
<th>X Coeff used</th>
<th>Scheme</th>
<th>Without attack PSNR</th>
<th>Without attack SSIM</th>
<th>Cropping attack PSNR</th>
<th>Cropping attack SSIM</th>
<th>Salt and pepper Noise PSNR</th>
<th>Salt and pepper Noise SSIM</th>
<th>Sharpening PSNR</th>
<th>Sharpening SSIM</th>
<th>Brightening PSNR</th>
<th>Brightening SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>X=5</td>
<td>Patra et al Proposed</td>
<td>36.9835 0.9261</td>
<td>36.973 0.9258</td>
<td>36.9000 0.9253</td>
<td>36.9931 0.9267</td>
<td>36.8015 0.9254</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X=10</td>
<td>Patra et al Proposed</td>
<td>36.2618 0.9195</td>
<td>36.3484 0.9200</td>
<td>36.2451 0.9193</td>
<td>36.2729 0.9185</td>
<td>36.3400 0.9199</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X=20</td>
<td>Patra et al Proposed</td>
<td>35.6821 0.9361</td>
<td>35.7596 0.9362</td>
<td>35.6833 0.9364</td>
<td>35.8105 0.9368</td>
<td>35.7496 0.9369</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X=30</td>
<td>Patra et al Proposed</td>
<td>35.4068 0.9481</td>
<td>35.4095 0.9497</td>
<td>35.4479 0.9484</td>
<td>35.4469 0.9479</td>
<td>35.4132 0.9789</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X=40</td>
<td>Patra et al Proposed</td>
<td>35.2375 0.9574</td>
<td>35.252 0.9565</td>
<td>35.3071 0.9582</td>
<td>35.2212 0.9578</td>
<td>35.2212 0.9578</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X=50</td>
<td>Patra et al Proposed</td>
<td>35.1516 0.9620</td>
<td>35.1801 0.9644</td>
<td>35.1109 0.9643</td>
<td>35.1126 0.9636</td>
<td>35.1986 0.9647</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X=60</td>
<td>Patra et al Proposed</td>
<td>35.0935 0.9694</td>
<td>35.0212 0.9691</td>
<td>35.0620 0.9710</td>
<td>35.062 0.9710</td>
<td>35.0799 0.9699</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table-3. TAF quality comparison between DCT and DTT based schemes.**

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Sharpen (50%)</th>
<th>Noise (Salt and Pepper)</th>
<th>Brighten (110%)</th>
<th>Without attack</th>
<th>crop</th>
<th>Compress (50%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patra et al</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

It was demonstrated that the SVD [10] [12] and CRT based spatial domain technique do not work for cropping, brighten, sharpen and compression operations. The proposed technique is better than SVD [10] [12] and CRT based, because it can withstand all aforementioned operations. Considering the case about the reconstructed watermarked image quality, our technique exhibit better visual quality than the other existing schemes [7] [21]. The improvement in SSIM value from Table-2 is a clear evidence of the reconstructed watermarked image quality. Table-4 shows the reconstructed watermark quality comparison under different attacks. It has been seen that the reconstructed image quality is robust to almost all attack.
complex (in time) than DCT scheme. However, it is trivial for hardware implementation as the DTT kernel coefficients can be implemented directly in hardware, like DCT kernel coefficients. As the correlation between the proposed scheme and CRT based DCT are similar in approach, we expect that by doubling the watermarking scheme, the imperceptibility and robustness against various attacks can be maintained. The proposed scheme can also be applied to text, audio and video.

REFERENCES


