ABSTRACT

In this paper a proficient digital watermarking strategy is proposed for copyright insurance. The proposed watermarking algorithm embed a binary logo watermark into main image additionally the security of logo is kept up by utilizing the chaotic maps after which it is transformed to DCT domain and then inserted into main image by detecting the suitable sub-band component in the wavelet domain. The horizontal and vertical wavelet components of level 2, 3 or higher depending upon the size of watermark are used to implant the digital watermark. The approach can successfully embed a greatly invisible watermark due to the perfect selection of embedding components in wavelet domain which perfectly exploits the limitations of human visual perception system. The watermark is recovered by (1) contrasting the relationships between the wavelet coefficients of watermarked image (2) the public key codes generated during embedding process and (3) the private key generated data. The experimental result shows the robustness of the proposed watermarking technique against different of image modification operations for example, compression, noise, and geometric operations.

Keywords--- Digital Watermark, Discrete Wavelet Transform (DWT), Chaotic Encryption, Discrete Cosine Transform (DCT)

I. INTRODUCTION

As the Internet turns into the principle mean of transferring and data, individuals concern about the copyright assurance of digital information has been increased greatly, especially for, visual and multimedia documents. At the point, digital watermarking strategies are continuously increasing, to get the tradeoff amongst three properties: information embedding capacity, detectability, and robustness against image processing operations [10]. The watermarking is done either on spatial domain or in transform domain. The decision of a domain lies mainly on robustness required and processing resource availabilities.

Between these domains the spatial shows much robust behavior against geometrical transforms [9]. In the other, hand its poor data embedding capability with respect to the detection possibilities limits its applicability. For example in LSB embedding technique, the few bit implanted in the host image which can be easily removed by simple image processing techniques. Numerous analysts have been concentrating on security and robustness [3], yet infrequently on the watermarking limit [4]. Surely, robustness and security will be key to acquire an irremovable and undetectable watermark; in any case, in the event that we can insert more information in the host image through mathematical transform, the applicability of watermark can be numerously increased in different areas. In the present work, anew strategy for spatial main water marking is presented which overcomes the restrictions of the ordinary spatial systems as LSB or CDMA [5]. The strategy utilizes a scrambled information to implant it through wavelet domain.

II. LITERATURE REVIEW

During the past few years, several information hiding techniques have been investigated extensively and great achievements have been obtained. However this paper focuses on robust watermarking. A good watermarking scheme should be able to retrieve the watermark even when the image is attacked by geometric distortions, such as image rotation and scaling. This section presents a brief review of literature found useful in order to achieve this goal. Romain Mavudila et al. [7] A combined dual-tree transform wavelet(DT-CWT) and Bivariate Shrinkage for medical image watermarking The main part of this paper is devoted to exploit the exceptional quality of DTT combined with Bi directional wavelet(DT-CWT) and Bivariate Shrinkage for medical image watermarking. The main part of this paper is devoted to exploit the exceptional quality of DTT combined with Bivariate Shrinkage with Local Variance Estimation at the extracted step of the watermark in the medical images. They also examined the security issues form edical data to protect these data in medical information. Yaoli Liu et al. [5] propose a robust
watermarking algorithm for medical image authentication and protection. The scheme obtains the visual feature vectors of the medical image using DWT-DCT. The watermarking image is encrypted by Logistic Map to strengthen its security. Alessandra Lumnini et al. [4] proposed a wavelet-based image watermarking scheme is proposed, based on the insertion of pseudo-random codes in the frequency domain. The original image is required for the watermark detection. Zhao Dawei et al. [6] presented a chaos-based watermarking algorithm is developed in the wavelet domain for still images. In contrast to the conventional approach, they applied the wavelet transform only locally. Then transform the sub-image, which is extracted from the original image, in the frequency domain by using DWT and then embed the chaotic watermark into part of the sub-band coefficients. Hui Zhang et al. [1] proposed a new watermarking approach which allows watermark detection and extraction under affine transformation attacks. The novelty of our approach stands on a set of affine invariants we derived from Legendre moments. Watermark embedding and detection are directly performed on this set of invariants. They also show how these moments can be exploited for estimating the geometric distortion parameters in order to permit watermark extraction. Hong Shen et al [8] proposes an effective approach to embed dual watermarks by extending the single watermarking algorithms in for numerical and logo watermarking, respectively.

III. WATERMARK ENCRYPTION

The proposed algorithm uses the two levels of encryption in this section explains the first level encryption which is used to encrypt the original watermark image using chaotic map. In recent years, chaotic maps have been used for digital watermarking, to increase the security [6]. The most attractive features of chaos in information hiding are its extreme sensitivity to initial conditions and the outspreading of orbits over the entire space. These special characteristics make chaotic maps excellent candidates for watermarking and encryption, based on the classic Shannon’s requirement of confusion and diffusion [6]. The Cat’s map also known as Arnold map is one of the simplest chaotic maps given by:

\[
\begin{pmatrix}
\bar{x} \\
\bar{y}
\end{pmatrix}
= \begin{pmatrix}
1 & 1 \\
1 & 2
\end{pmatrix}
\begin{pmatrix}
x \\
y
\end{pmatrix} \mod N, \ldots, \ldots, (1)
\]

The values of square matrix \(\begin{pmatrix} 11 \\ 12 \end{pmatrix}\) used in above equation can be used as key to encryption and decryption.

At the second level of encryption the Logistic map is used because at this level only one dimensional data is needed. Logistic map is described by:

\[
x_{k+1} = \mu x_k (1 - x_k), \ldots \ldots \ldots \ldots (2)
\]

Where \(0 \leq \mu \leq 4\). When \(3.5699456 \leq \mu \leq 4\), the map is in the chaotic state. A sequence generated by the logistic map will be used to generate the public key.

4. THE DISCRETE WAVELET TRANSFORM (DWT)

The wavelet transform, first proposed by S. Mallat in 1988, is a new signal analysis the or yandisa “time-frequency” method[5]. The basic idea of DWT is to analyse the signal \(f(t)\) based on wavelet function \(\psi_{a,b}(t)\):

\[
W_{f,a,b} = \int_{R} f(t) \bar{\psi}_{a,b}(t) dt, \ldots \ldots \ldots \ldots (3)
\]

Where, wavelet function \(\psi_{a,b}(t)\) is a group of functions obtained from the same basic function \(\psi\) by translating and stretching.

\[
\psi_{a,b}(t) = a^{1/2} \psi \left( \frac{t-a}{b} \right), a, b \in R, a \neq 0, \ldots \ldots \ldots \ldots (4)
\]

Where, \(\psi\) is the dilated function, \(a\) and \(b\) are the dilation factor and the translation factor, respectively. The decomposing equation of the Mallat algorithm is as follows:

\[
c_{j+1,k} = \sum_{n \in Z} c_{j,n} h_{n-2k}, k \in R, \ldots, \ldots \ldots \ldots (5)
\]

\[
d_{j+1,k} = \sum_{n \in Z} c_{j,n} g_{n-2k}, k \in Z, \ldots, \ldots \ldots \ldots (6)
\]

The reconstruction equation of the Mallat algorithm is given by:

\[
c_{j,k} = \sum_{n \in Z} c_{j,n} h_{n-2k} + \sum_{n \in Z} c_{j,n} g_{n-2k}, k \in Z, \ldots \ldots \ldots \ldots (7)
\]

By the one-layer wavelet decomposition of the two-dimensional signal image, four sub-band image can be acquired. Where, \(L_{H_{1}}\) is the approximated subband image with low frequency characteristics. The others \((L_{H_{1}}, L_{H_{1}}, and H_{H_{1}})\) with high frequency characteristics.

IV. THE DISCRETE COSINE TRANSFORM (DCT)

DCT for image coding is the standard of the Joint Photographic Experts Group (JPEG) and new Moving Picture Experts Group (MPEG). It is well known for the best balance between operation speed and high precision of extracting the feature vector. The \(M \times N\) medical image's DCT is defined by:

\[
F(u, v) = c(u) c(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \frac{\cos(\pi(2x + 1)u) \cos(\pi(2y + 1)v)}{2M} \frac{2N}{2N}, \ldots \ldots \ldots \ldots (9)
\]

\(u = 0, 1, \ldots, M - 1; v = 0, 1, \ldots, N - 1\)
Step 6: Scramble the watermark signal with Arnold map using given frequency domain sampling. Digital image pixels are usually square, i.e. $M = N$.

V. PROPOSED ALGORITHM

The main strength of the proposed transform domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of spatial domain or to support additional features. Watermarking process is started by applying 3-levels DWT on the host image. The agreement adopted by many DWT-based watermarking methods is to embed the watermark in the middle frequency sub-bands $H_{Lx}$ and $L_{Hx}$ is better in perspective of imperceptibility and robustness. Consequently, $H_{Lx}$ coefficient sets in level three is chosen to make in crease the robustness of our watermark against common watermarking attack, specially three is chosen to make in crease the robustness of our watermark.

V. PROPOSED ALGORITHM

Step 1: Perform DWT on the host image to decompose it into four non-overlapping multi-resolution coefficient sets: $LL$, $HL$, $LH$ and $HH$.

Step 2: Perform DWT again on two $HL$ and $LH$ coefficient sets to get eight smaller coefficient sets and choose four coefficient sets: $H_{LLx}, H_{LHx}, L_{Hlx}$, and $L_{LHx}$.

Step 3: Perform DWT again on four coefficient sets: $H_{LHx}, H_{LLx}, L_{Hlx}$, and $L_{LHx}$ to get sixteen smaller coefficient sets and choose four coefficient sets: $H_{LLx}, H_{LHx}, L_{Hlx}$, and $L_{LHx}$.

Step 4: Divide four coefficient sets: $H_{LHx}, H_{LLx}, L_{Hlx}$, and $L_{LHx}$ into $4 \times 4$ blocks.

Step 5: Perform DCT to each block in the chosen coefficient sets.

Step 6: Calculate the average of each DCT block. Now generate a binary sequence by comparing the subsequent blocks value as follows:

$$B(i) = \begin{cases} 1, & \text{if } Blk_{\text{avg}}(i) - Blk_{\text{avg}}(i + 1) > th \\ 0, & \text{otherwise} \end{cases}$$

Step 6: Scramble the watermark signal with Arnold map using given $key_1$ and gain the shuffled watermark $W'$, key times can be seen as private key.

Step 7: now XOR the $B$ with $W'$ to get the temporary public key.

$$Pub_{temp} = XOR(B, W')$$

Step 8: Generate a binary sequence ($L$) of length equal to $Pub_{temp}$ by Logistic map using given $key_2$ and XOR it with $Pub_{temp}$ to gain the final private key.

$$Pub_{final} = XOR(Pub_{temp}, L)$$

Step 9: Perform in verse DCT(IDCT) on each block after its mid-band coefficients have been modified to embed the watermark bits as described in the previous step.

Step 10: Perform the inverse DWT (IDWT) on the DWT transformed image, including the modified coefficient sets, to produce the watermarked host image.

To extract we need just to perform in opposite direction hence no separate explanation is required.

VI. EXPERIMENTAL RESULTS

For the testing of the proposed algorithm following measures are used for assessment of quality of image and watermark.

6.1 MEAN ABSOLUTE ERROR (MAE):

It is a quantity used to measure how close forecasts or predictions are to the eventual outcomes. The mean absolute error is given by

$$MAE = \frac{1}{n} \sum_{i=1}^{n} |f_i - y_i| = \frac{1}{n} \sum_{i=1}^{n} |e_i|$$

As the name suggests, the mean absolute error $e_i = |f_i - y_i|$ is an average of the absolute errors, where $f_i$ is the prediction and the true value. Note that alternative formulations may include relative frequencies as weight factors. The mean absolute error is a common measure of forecast error in time series analysis, where the terms "mean absolute deviation" is sometimes used in confusion with the more standard definition of mean absolute deviation. The same confusion exists more generally.

6.2 PEAK SIGNAL-TO-NOISE RATIO (PSNR):

It is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. It is most easily defined via the mean squared error (MSE) which for two $m \times n$ monochrome images $I$ and $K$ where one of the images is considered a noisy approximation of the other is defined as:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

$$PSNR = 20 \cdot \log_{10} \left( \frac{MAX_I}{\sqrt{MSE}} \right) = 20 \cdot \log_{10} \left( \frac{MAX_I}{\sqrt{MSE}} \right) = 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$
Here, $MAX_i$ is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

The proposed algorithm has been extensively tested on various standard images, and the summarized results are presented in tabular form.

![Cover images used for the experiment Cameraman, Lena and Barbara.](image)

6.3 EXPERIMENTAL RESULTS UNDER NON-ATTACKED:

![Cover images with embedded watermarks](image)

![Recovered Watermarks](image)

<table>
<thead>
<tr>
<th>Images</th>
<th>PSNR</th>
<th>MAE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cameraman</td>
<td>37.88</td>
<td>0.026</td>
</tr>
<tr>
<td>Lena</td>
<td>37.26</td>
<td>0.032</td>
</tr>
<tr>
<td>Barbara</td>
<td>37.45</td>
<td>0.014</td>
</tr>
</tbody>
</table>

Table 1: Experimental results under Non-Attacked

<table>
<thead>
<tr>
<th>Scaling%</th>
<th>Image</th>
<th>MAE</th>
</tr>
</thead>
<tbody>
<tr>
<td>25%</td>
<td>Barbara</td>
<td>0.12</td>
</tr>
<tr>
<td></td>
<td>Baboon</td>
<td>0.16</td>
</tr>
<tr>
<td></td>
<td>Peppers</td>
<td>0.11</td>
</tr>
<tr>
<td>50%</td>
<td>Barbara</td>
<td>0.22</td>
</tr>
<tr>
<td></td>
<td>Baboon</td>
<td>0.24</td>
</tr>
<tr>
<td></td>
<td>Peppers</td>
<td>0.18</td>
</tr>
</tbody>
</table>

Table 3: Results for Scaling Attack

<table>
<thead>
<tr>
<th>Compression Ratio</th>
<th>Image</th>
<th>MAE</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Barbara</td>
<td>0.023</td>
</tr>
<tr>
<td></td>
<td>Baboon</td>
<td>0.026</td>
</tr>
<tr>
<td></td>
<td>Peppers</td>
<td>0.012</td>
</tr>
<tr>
<td>10</td>
<td>Barbara</td>
<td>0.082</td>
</tr>
<tr>
<td></td>
<td>Baboon</td>
<td>0.063</td>
</tr>
<tr>
<td></td>
<td>Peppers</td>
<td>0.069</td>
</tr>
</tbody>
</table>

Table 4: Results for JPEG Compression Attack

6.3 NOISE ATTACK

Table 2: Results for Salt and Pepper Attack

<table>
<thead>
<tr>
<th>Noise Density</th>
<th>Image</th>
<th>MAE</th>
</tr>
</thead>
<tbody>
<tr>
<td>$d = 0.05$</td>
<td>Cameraman</td>
<td>0.036</td>
</tr>
<tr>
<td></td>
<td>Lena</td>
<td>0.061</td>
</tr>
<tr>
<td></td>
<td>Barbara</td>
<td>0.027</td>
</tr>
<tr>
<td>$d = 0.10$</td>
<td>Cameraman</td>
<td>0.072</td>
</tr>
<tr>
<td></td>
<td>Lena</td>
<td>0.083</td>
</tr>
<tr>
<td></td>
<td>Barbara</td>
<td>0.043</td>
</tr>
</tbody>
</table>

6.4 SCALING ATTACK

VII. CONCLUSION

Our study on this focused on presenting a joint DWT-DCT domain digital image watermarking algorithm protected by two level of encryption. The proposed method exploits strength of two common transforms; DCT and DWT, to obtain further imperceptibility and robustness. The idea of inserting watermark in the combined transform is based on the fact that they can complement each other for eliminating their limitations. The experimental results show that the imperceptibility of the watermarked image is acceptable and does not show any sign on insertion during normal visible inspection. The presented method is also tested for most of the common image processing attacks and the results show that that proposed method is very robust and even after increasing the intensity of attack the watermark remains recoverable. On the further development we can develop the efficient technique to reduce the computational complexity by utilizing the characteristics of transforms and image.

REFERENCES
