II. CLASSIFICATION OF DIGITAL WATERMARK

- DIGITAL WATERMARK
  - Human Perception
  - Application
  - Document
    - Visible
    - Invisible
    - Robust
    - Text
    - Audio
    - Fragile
    - Semi-Fragile
    - Video
    - Image

Visible Watermark — The information is visible in the multimedia. It may be a text or a logo, for identification of the owner.

Invisible Watermark — The information here is Hidden and cannot be seen to validate the owners authentication.

Robust Watermark — It is mainly used to sign copyright information of the digital works [4], the embedded watermark can resist the common edit processing, image processing and lossy compression, the watermark is not destroyed after some attack and can still be detected to provide certification.

Fragile Watermark — Fragile watermarks are those watermarks which can be easily destroyed by any attempt to tamper with them. Fragile watermarks are destroyed by data manipulation.

Semi-Fragile Watermark — These are sensitive to signal modification. Contains feature of both robust & fragile watermark. Provides data authentication.

III. DIGITAL WATERMARKING TECHNIQUE

A watermarking algorithm embeds a visible or an invisible watermark in a given multimedia object. The embedding process is supervised by use of a secret key which decides the locations within the multimedia object to which part the watermark would be embedded. Once the watermark is embedded into the object, it may experience several attacks because the multimedia object can be digitally processed. The attacks may or may not be intentional (like cropping).
Hence the watermark embedded has to be very robust against all these possible attacks. When the owner checks for the attacked and distorted watermarked object, s/he relies on the secret key that was used to embed the watermark. Using the secret key, the embedded watermark sequence can be extracted.

A. Architecture of Digital Watermarking

Watermark embedding embeds the watermark into the original work using a key.

![Watermark embedding module]

**Figure 1:** Watermark embedding module

Watermark detection and extraction module is used to determine whether the data contains specified watermark or the watermark can be extracted.

![Watermark detection module]

**Figure 2:** Watermark detection and extraction module

IV. WATERMARKING APPROACHES

Digital watermarking system can be classified into two main domains i.e. Spatial domain techniques and Frequency domain techniques [5].

In spatial domain class generally have following characteristics [4, 8]:

1) The watermark is applied in the pixel domain.
2) No transforms are applied to the host signal during watermark embedding.
3) Combination with the host signal is based on simple operations, in the pixel domain.
4) The watermark can be detected by correlating the expected pattern with the received signal.

<table>
<thead>
<tr>
<th>Watermarking Domains</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spatial</td>
<td>Least Significant Bit Coding</td>
</tr>
<tr>
<td></td>
<td>Correlation Based</td>
</tr>
<tr>
<td></td>
<td>Predictive Coding</td>
</tr>
<tr>
<td></td>
<td>Spread Spectrum Based [9]</td>
</tr>
<tr>
<td>Frequency</td>
<td>Discrete Cosine Transform(DCT)</td>
</tr>
<tr>
<td></td>
<td>Spread Spectrum</td>
</tr>
<tr>
<td></td>
<td>Discrete Wavelet Transform and related techniques (DWT)</td>
</tr>
<tr>
<td></td>
<td>Discrete Fourier Transform (DFT)</td>
</tr>
<tr>
<td></td>
<td>Combination of DWT and DCT</td>
</tr>
</tbody>
</table>

Discrete cosine transforms (DCT): DCT based watermarking techniques are more robust technique compared to simple spatial domain watermarking techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, it is difficult to implement them and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT is used in the most popular stills and video compression formats, including JPEG, MPEG, and H.26x [3]. This allows the integration of both watermarking and compression into a single system.

Steps in DCT Block Based Watermarking Algorithm

1) Segment the multimedia into non-overlapping blocks of 8x8
2) Apply forward DCT to each of these blocks
3) Apply some block selection criteria (e.g. HVS)
4) Apply coefficient selection criteria (e.g. highest)
5) Embed watermark by modifying the selected coefficients.
6) Apply inverse DCT transform on each block.

**Discrete wavelet transforms (DWT):** DWT is more efficient than DCT transform method. A two level DWT decomposes image into low and high frequency components. Embedding the watermark in low frequencies obtained by wavelet decomposition increases the robustness with respect to various attacks. Here first media is divided into frames. Then luminance component of each frame is chosen and DWT is applied to it which results into different sub bands. These bands are again divided into different parts. For each part covariance matrix is calculated. By applying inverse DWT watermarked luminance component of the frames are obtained. Finally by reconstructing the watermarked frame watermarked media is obtained.

**Advantages of DWT over DCT:** In Wavelet transform the HVS are more closely processed than the DCT. Wavelet coded object is a multi-resolution description of object. Hence any media can be shown at different levels of resolution and can be processed sequentially from low resolution to high resolution.

**Disadvantages of DWT over DCT:** Computational complexity of DWT is more compared to DCT. As Feig (1990) pointed out it only takes 54 multiplications to compute DCT for a block of 8x8, unlike wavelet calculation depends upon the length of the filter used, which is at least 1 multiplication per coefficient [10].

**Discrete Fourier Transform (DFT):** It transforms a continuous function into its frequency domain. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT shows translation invariance.

Spatial shifts in the multimedia affects the phase representation of it but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform [7].

**Advantages of DFT over DWT and DCT:** DFT has an advantage of rotation, scaling and translation (RST) invariance. Hence it can be useful in recovering from geometric distortions, whereas the spatial domain, DCT and the DWT are not RST invariant and hence it is difficult to overcome from geometric distortions.

| TABLE II Comparison of Watermarking techniques [2]. |
|-----------------|-----------------|-----------------|
| **Factors**     | **Spatial Domain** | **Frequency Domain** |
| Computation Cost| Low              | High            |
| Robustness      | Fragile          | More Robust     |
| Perceptual quality | High control   | Low control     |
| Computational complexity | Low          | High            |
| Computational Time | Less           | More            |
| Capacity        | High             | Low             |
| Example Application | Mainly         | Authentication  |

V. **DIGITAL WATERMARKING PROPERTIES**

**Effectiveness** -- This is the probability that the message in a watermarked media will be correctly detected.

**Fidelity** -- Watermarking is a process that alters an original media to add a message to it, therefore it inevitably affects the media’s quality.

**Payload Size** -- Every watermarked work is used to carry a message. The size of this message is often important as many systems require a relatively big payload to be embedded in a cover work.

**Robustness** -- There are many cases in which a watermarked work is altered during its lifetime, either by transmission over a lossy channel or several malicious attacks that try to remove the watermark or make it undetectable.

VI. **ATTRIBUTES OF DIGITAL WATERMARKING**

**A. Copyright Protection**

Digital watermarks can be used to identify and protect copyright ownership.

**B. Copy Protection**

Digital content can be watermarked to indicate that the content cannot be illegally replicated. Devices capable of replication can then detect such watermarks and prevent unauthorized replication of the content.

**C. Tracking**

Digital watermarks can used to track the usage of digital content. Each copy of digital content can be uniquely watermarked with data specifying the authorized users of the content.
Such watermarks can be used to detect illegal replication of content by identifying the users who replicated the content illegally. The watermarking technique used for tracking is called as fingerprinting.

**D. Broadcast Monitoring**

Digital watermarks can be used to monitor broadcasted content like television and broadcast radio signals. Advertising companies can use systems that can detect the broadcast of advertisement for billing purposes by identifying the watermarks broadcast along with the content.

**E. Meta-data Insertion**

It refers to the data that describes data. Multimedia can be labelled with its content and can be used in search engines. Audio files can carry the lyrics or the name of the singer or the site from where they are being loaded. Medical X-rays could store patient records.

**F. Digital Fingerprinting**

It is a technique used for detection of the owner of the digital content. Fingerprints are unique to the owner of the digital content. Hence a single digital object can have different fingerprints because they belong to different users.

**VII. CONCLUSION**

This paper briefly describes about digital watermarking and its techniques. It also, shows the comparison of various watermarking techniques and their advantages and disadvantages in various aspects.

**REFERENCES**


