Abstract- In this paper, we describe a new very accurate and reliable method that can detect watermarked image by LSB embedding in randomly scattered pixels in both 24-bit color images and 8-bit grayscale or color images, the LSB Modification and DCT are two techniques are analyzed by using various distortion metrics the methods for their robustness.

Keywords— Image watermarking, Discrete Cosine Transform, Least Significant Bit technique, Robustness

I. INTRODUCTION

Watermark is a “secret message” that is embedded into a “cover (original or host) message”. Only the knowledge of a secret key allows us to extract the watermark from the cover message. Effectiveness of a watermarking algorithm is a function of it’s:

1. Resilience to attacks
2. Capacity
3. Stealth

Watermarking is very similar to steganography in a number of aspects. Both seem to embed information inside a cover message with little or no degradation of the cover media. Watermarking however adds the additional requirement of robustness. An ideal steganographic system would securely add large amount of information to the cover media without causing any visual degradation. Whereas an ideal watermarking system would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. A watermarking system would thus trade capacity and even security for additional robustness.

II. TYPES OF WATERMARKING

1. Visible watermarking
2. Invisible watermarking

A Visible watermark is a visible translucent image which is overlaid on the primary image. Perhaps consisting of the logo or seal of the organization which holds the rights to the primary image, it allows the primary image to be viewed, but still marks it clearly as the property of the owning organization. It is important to overlay the watermark in a way which makes it difficult to remove, if the goal of indicating property rights is to be achieved. An example shows both a watermark and an image with the watermark overlaid.

An invisible watermark is an overlaid image which cannot be seen, but which can be detected algorithmically. The invisibility is assured by inserting a watermark and a secret key to form a composite watermarked signal. Hiding information, where electronic media are used as such carriers, requires alterations of the media properties may introduce some form of degradation. If applied to images that degradation, at times, may be visible to the human eye and point to signatures of the watermarking methods and tools used. These signatures may actually broadcast the existence of the embedded message purpose of watermarking, which is hiding the existence of a message.
approach, the relative easiness to implement it, makes it a popular method. To hide a secret message inside a image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24 bit color image, a bit of each of the red green and blue color components can be used, so a total of 3 bits can be stored in each pixel. Thus, a 800 × 600 pixel image can contain a total amount of 1,440,000 bits (180,000 bytes) of secret data.

Figure 2. LSB Modification Watermarking

III. PROBLEM SPECIFICATION

There are numerous watermarking methods till date, which can be classified, as described earlier, according to the method of embedding of data inside the medium. All these methods vary mostly in the prospect of providing robustness against attacks, both intentional and unintentional. Here we present two of the most prevalent approaches, and their detailed analysis with the various benchmarks specified. The two methods are:

1. LSB Modification: The most widely used technique to hide data is the usage of the LSB. Although there are several disadvantages to this approach, the relative easiness to implement it, makes it a popular method. To hide a secret message inside a image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm.

2. Spread spectrum Technique: Spread-spectrum telecommunications is a signal structuring technique that employs direct sequence, frequency hopping, or a hybrid of these, which can be used for multiple access and/or multiple functions. This technique decreases the potential interference to other receivers while achieving privacy. Spread spectrum generally makes use of a sequential noise-like signal structure to spread the normally narrowband information signal over a relatively wideband band of frequencies.

The above two techniques are analysed by using various distortion metrics to verify the methods for their robustness. Standard test images like Lenna etc. have been used and the analysis results have been limited to images of Human Faces (or similar type), and the final observations tabulated and a conclusion made.

IV. LSB MODIFICATION TECHNIQUE

The most widely used technique to hide data, is the usage of the LSB. Although there are several disadvantages to this method, the relative easiness to implement it, makes it a popular method. To hide a secret message inside a image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24 bit color image, a bit of each of the red green and blue color components can be used, so a total of 3 bits can be stored in each pixel. Thus, a 800 × 600 pixel image can contain a total amount of 1,440,000 bits (180,000 bytes) of secret data.

\[
B(k) = \sum_{i=0}^{N-1} A(i) \cos \left( \frac{\pi k i}{N} \right) \frac{(2i+1)}{2}
\]

The above formula is defined for all values of the frequency-space.
variable k, but we only care about integer k in the range 0 to N-1. **The inverse DCT** (which would be used e.g. by a decoder) is:

\[ A(i) = \sum_{k=0}^{N-1} B(k)(2 \cdot \delta(k-0)) \cos\left(\frac{\pi k}{N}(2i+1)/2\right) \]

Where \( \delta(k) \) is the Kronecker delta.

The Discrete Fourier Transform (DFT) and Discrete Cosine Transform (DCT) perform similar functions: they both decompose a finite-length discrete-time vector into a sum of scaled-and-shifted basis functions. The difference between the two is the type of basis function used by each transform; the DFT uses a set of harmonically-related complex exponential functions, while the DCT uses only (real-valued) cosine functions.

**VI. DISTORTION METRICS**

The watermark robustness depends directly on the embedding strength, which in turn influences the visual degradation of the image. For fair benchmarking and performance evaluation, the visual degradation due to the embedding is an important and unfortunately often neglected issue. Since there is no universal metric, we review in this section the most popular pixel-based distortion criteria and introduce one metric, which makes use of the effect in the human visual system (HVS).

**VIII. DIFFERENT TYPES OF NOISE**

1. Gaussian
2. Localvar
3. Poisson
4. Salt & pepper
5. Speckle

**Gaussian noise** is a statistical noise that has its probability density function equal to that of the normal distribution, which is also known as Gaussian distribution. It having constant mean and variance. Gaussian noise is most commonly used to yield additive white Gaussian noise.

**Localvar noise** having Zero-mean Gaussian white noise with an intensity-dependent variance.

**Poisson noise** arises from Poisson processes. It applies to various phenomena of discrete properties whenever the probability of phenomena happening it constant in time or space.

**Salt & pepper noise** is a form of noise typically seen on images. It represents itself as randomly occurring white and black pixels.

**Speckle noise** is a granular noise that inherently exists in and degrades the quality of the active radar and synthetic aperture radar (SAR) images.

Speckle noise in conventional radar results from random fluctuation in the return signal from an object that is no bigger than a single image processing element. It increases the mean grey level of a local area.

**IX. APPLICATION AREAS**

There are many applications for digital watermarking of images, including copyright protection, feature tagging, and secret communication:

1. **Fingerprinting**: An owner can embed a watermark into his content that identifies the buyer of the copy (e.g., serial number). If unauthorized copies are found later, the owner can trace the origin of the illegal copies.

2. **Authentication**: The creator of content can embed a **fragile watermark** into the content to provide a proof of authenticity and integrity. Any tampering of the original content destroys the fragile watermark and thus can be detected.

3. **Feature Tagging**: Captions, annotations, time stamps, and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features. In an image database, keywords can be embedded to facilitate search engines. If the image is a frame of a video sequence, timing markers can be embedded in the image for synchronization with audio. The number of times an image has been viewed can be embedded for “pay-preview” application.

4. **Copyright Protection**: When an image is sold or distributed an identification of the recipient and time stamp can be embedded to identify potential pirates. A watermark can also serve to detect whether the image has been subsequently modified. Detection of an embedded watermark is performed by a statistical, correlation, or similarity test, or by measuring other quantity characteristic to the watermark in a stego-image. The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent surge of interest in digital watermarking and data embedding.

5. **Secret Communications**: In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be restricted or forbidden by law. However, the use of steganography does not advertise covert communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers or eavesdroppers.

6. **Ownership assertion**: A rightful owner can retrieve the watermark from his content to prove his ownership.
X. RESULT
Watermarked image

Watermarked and noised image

Recovered watermark

Recovered watermark and noise

Histogram of image before watermarking and after watermarking

XI. CONCLUSION
In this paper, an analysis for image watermarking has been presented. We recover watermarked image with noise and without noise by the use of LSB modification and DCT. The analysis embeds the watermark code by LSB modification and DCT of the image, and exploits a model derived from image compression techniques for adapting the watermark strength to the characteristics of the HVS. The performances of the novel algorithm are very good, experimental results, in fact, supported the suitability of DCT watermarking schemes for robustly hiding watermarks into images. In particular, the behavior of the watermark detector with respect to image cropping was surprisingly good. As a matter of fact, DCT schemes do not spread the watermark all over the image, but, the watermarking energy can be kept so high that even a small portion of the image is sufficient to
correctly guess the embedded code. As Watermarking becomes more widely used in computing there are issues that need to be resolved. There are a wide variety of different techniques with their own advantages and disadvantages.

REFERENCES