A SCHEME OF WATERMARKING USING NEW DCT ALGORITHM FOR IMAGE COPYRIGHT PROTECTION

Bankar M.A, 2Bankar S. K, 3Gavi S.B, 4Vyawahare J. S & 5Nalawade V. S

Department Of Computer Engineering,
SBPCOE, Indapur, India

1minalbankar@gmail.com, 2Sbbankar63@gmail.com, 3gavisoniya@gmail.com,
4jyotivyawahare@gmail.com, 5Vinaynalawade2007@gmail.com

Abstract- The risk of copyright violation of multimedia data has increased due to the enormous growth of computer networks that provides fast and error free transmission of any unauthorized duplicate and possibly manipulated copy of multimedia information. One possible solution may be to embed a secondary signal or pattern into the image that is not perceivable and is mixed so well with the original digital data that it is inseparable and remains unaffected against any kind of multimedia signal processing. This embedded secondary information is digital watermark which is, in general, a visible or invisible identification code that may contain some information about the intended recipient, the lawful owner or author of the original data, its copyright etc. in the form of textual data or image. This idea describes overview of digital image watermarking technique and proposed scheme to make a basic watermarking algorithm based on Discrete Cosine Transformation (DCT) for protecting digital images. The proposed watermarking algorithm first read the original image then computes the DCT of original image and simultaneously going to read the secret message or watermark image. This watermarking image is embedded in to original image. Finally with the help of watermarking algorithm add the secret message in to original image. Also this proposed algorithm is used for copy write protection of digital images in DCT domain.

Keywords- Discrete cosine transform (DCT), copyright protection, Digital image watermarking.

I. INTRODUCTION

With digital multimedia distribution over World Wide Web, authentications are more threatened than ever due to the possibility of unlimited copying. So, watermarking techniques are proposed for copyright protection or authentication of digital media. The types of protection systems involve the use of both encryption and authentication techniques. These digital watermarks also offer forgery detection. Thus security of multimedia contents becomes a vital issue and there is a need in protecting the digital content against counterfeiting, piracy and malicious manipulations. Digital watermarking is an evolving field that requires continuous effort to find for the best possible method in protecting multimedia content. During recent years, digital watermarking has drawn a lot of attention as a solution of this problem. In general, a digital watermarking algorithm tries to adhere some copyright information to the original data. Although watermarks can be visible, invisible watermarks are usually referred.

Digital images are now widely distributed on the Internet and via CD-ROM. Digital imaging allows an unlimited number of copies of an “original” to be easily distributed and/or forged. This presents problems if the image is copyrighted. The protection and enforcement of intellectual property rights has become an important issue in the “digital world.” Many approaches are available for protecting digital data; traditional methods include encryption,
authentication and time stamping. In this scheme algorithms for image authentication and forgery prevention known as digital watermarks Techniques of embedding a secret imperceptible signal, directly into the original data in such a way that always remains present, called watermark. Digital watermarking is an adaptation of the commonly used and well-known paper watermarks to the digital world.

II. PROPERTIES OF WATERMARKING

There are a number of important characteristics that a watermark can exhibit. These include that the watermark is difficult to notice, survives common distortions, resists malicious attacks, carries many bits of information, can coexist with other watermarks, and requires little computation to insert or detect. The relative importance of these characteristics depends on the application. The characteristics are discussed in more detail next.

A. Fidelity

The watermark should not be noticeable to the viewer nor should the watermark degrade the quality of the content. In earlier work, we had used the term imperceptible”, and this is certainly the ideal. However, if a signal is truly imperceptible, then perceptually based lossy compression algorithms either introduce further modifications that jointly exceed the visibility threshold or remove such a signal.

B. Robustness

Music, images and video signals may undergo many types of distortions. Lossy compression has already been mentioned, but many other signal transformations are also common. For example, an image might be contrast enhanced and colors might be altered somewhat, or an audio signal might have its bass frequencies amplified. In general, a watermark must be robust to transformations that include common signal distortions as well as digital-to-analog and analog-to-digital conversion and lossy compression.

C. Key restrictions

An important distinguishing characteristic is the level of restriction placed on the ability to read a watermark. As explained in earlier sections, we describe watermarks in which the key is available to a very large number of detectors as “unrestricted-key” watermarks, and those in which keys are kept secret by one or a small number of detectors as “restricted-key” watermarks.

D. Modification and multiple watermarks

In some circumstances, it is desirable to alter the watermark after insertion. For example, in the case of digital videodiscs, a disc may be watermarked to allow only a single copy. Once this copy has been made, it is then necessary to alter the watermark on the original disc to prohibit further copies. Changing a watermark can be accomplished by either (i) removing the watermark and then adding a new one or (ii) inserting a second watermark such that both are readable, but one overrides the other.

E. Data payload

Fundamentally, the data payload of a watermark is the amount of information it contains. As with any method of storing data, this can be expressed as a number of bits, which indicates the number of distinct watermarks that might be inserted into a signal. If the watermark carries N bits, then there are 2N different possible watermarks. It should be noted, however, that there are actually 2N + 1 possible values returned by a watermark detector, since there is always the possibility that no watermark is present.

F. Computational cost

As with any technology intended for commercial use, the computational costs of inserting and detecting watermarks are important. This is particularly true when watermarks need to be inserted or detected in real-time video or audio.

III. ATTACKS ON WATERMARKS

According to the watermarking jargon, an attack is any processing that may mess up detection of the watermark or communication of the information provided by the watermark. The processed, watermarked data is then called attacked data. Robustness against attacks is an important issue for watermarking schemes. The
usefulness of an attacked data can be measured by its perceptual quality and the amount of watermark destruction can be measured by criteria such as miss probability, probability of bit error, or channel capacity. An attack may succeed in defeating a watermarking scheme if it distorts the watermark beyond tolerable limits while maintaining the perceptual quality of the attacked data. Fig. 1 summarizes different types of attacks.

A. Removal attacks
These are the attacks that try to weaken or completely remove a watermark from its associated content, still preserving the content so that it is not useless after the attack is over. This category includes denoising, quantization, remodulation, and collusion attacks. Denoising and quantization attacks damage the watermark quality as much as possible, while keeping the quality of the attacked data high enough. The remodulation attack intends to predict the watermark. It may be implemented by subtracting the median filtered version of the watermarked image from the watermarked image itself.

B. Geometric attacks
Geometric attacks consist of the distortions particular to videos and images including operations as rotation, scaling, translation, cropping etc. In contrast to removal attacks, geometric attacks do not actually remove the embedded watermark, but attempt to deform the watermark detector synchronization with the embedded information. The embedded watermark information can be recovered if the perfect synchronization is regained.

C. Cryptographic attacks
Cryptographic attacks intend to break the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed deceptive watermarks. Brute-force search for the embedded secret information is one such technique. Another attack in this category is the so-called Oracle attack, which can be used to generate a non-watermarked signal when a watermark detector device is available. High computational complexity has restricted attackers from applying these attacks on watermarks.

D. Protocol attacks
Craver et al. mentioned an attack, called the watermark inversion attack or IBM attack, which produces a fake watermarking schemes that can be applied on a watermarked image to create doubt about which watermark was inserted first. Copy attack is another kind of protocol attack. In this case, the watermark is predicted by using a watermarked data, and this predicted watermark is embedded into another data by adapting the local features to satisfy its imperceptibility.

Fig. 1 Different attacks on watermark
IV. DIGITAL WATERMARKING SYSTEM

The digital watermarking system essentially consists of a watermark encoder and a watermark decoder (see Fig 2). The watermark encoder inserts a watermark onto the host signal and the watermark decoder detects the presence of watermark signal. Note that an entity called watermark key is used during the process of embedding and detecting watermarks. The watermark key has a one-to-one correspondence with watermark signal (i.e., a unique watermark key exists for every watermark signal). The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. Further, note that the communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital watermarking techniques should be resilient to both noise and security attacks. Fig. 2 illustrates the digital watermark methodology.

A. The Encoder Process

Let us denote an image by $f$, a key by $Key = key_1, key_2$, and the watermarked image by $WI$. $E$ is an encoder function, it takes an image $f$ and a key $Key$, and it generates a new image which is called watermarked image $WI$, mathematically,

$$E( f, Key ) = WI. \tag{1}$$

It should be noted that the key may be dependent on image. In such cases, the encoding process still holds.

B. The Decoder Process

A decoder function $D$ takes an image $J$ (which can be a watermarked or un-watermarked image, and possibly corrupted) whose ownership is to be determined and recovers a signature from the image. In this process an additional image $I$ can also be included which is often the original and un-watermarked version of $J$. This is due to the fact that some encoding schemes may make use of the original images in the watermarking process to provide extra robustness against intentional and unintentional corruption of pixels. Mathematically,

$$D( J, f ) = S. \tag{2}$$

The extracted signature $S$ will then be compared with the owner signature sequence by a comparator function.

V. WHY PREFERENCE TO DCT

1) In spite of the fact that the Karhunen-Loeve transform is an optimal transform in the image packing sense the DCT is more practical as the computational complexity involved in the DCT is much less compared to the K-L transform. The sinusoidal transforms like the DCT closely approximate the information packing ability of the optimal K-L transform.

2) The image packing ability of the discrete cosine transform is much superior to the discrete Fourier transform and the Walsh-Hadamard transform. This results in better image utility and storage.

3) The DCT has many other advantages as follows:
   a) It has been implemented in a single integrated circuit.
   b) It enables the user to pack most information in the fewest coefficients (for most natural images).

Furthermore, the sensitivity of the HVS to the DCT based images has been extensively studied, which resulted in the recommended JPEG quantization Table. These results can be used for predicting and minimizing the visual impact of the distortion caused by the watermark. Finally, the block-based DCT is widely used for image and video compression. By embedding a watermark in the same domain as the compression scheme used to process the image, we can anticipate lossy compression because we are able to anticipate which DCT coefficients will be discarded by the compression scheme.
VI. METHODOLOGIES

Discrete Cosine Transform (DCT):
The discrete cosine transform is a Fourier related transform similar to the discrete transform, but using only real numbers. It is equivalent to a discrete Fourier transform (DFT) of roughly twice the length, operating on real data with even symmetry. There are multiple advantages to using the DCT over even fast Fourier transform (FFT) for application purposes. The first main advantage of DCT is its efficiency. As the size of image to be produced increases, the FFT becomes increasing complex at much more rapid rate, and is not efficient for compression. A transformation function, which transforms the representation of data from space domain to frequency domain. The two-dimensional DCT of an M-by-N image A is defined as follows:

\[ A_{p,q} = \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos \left( \frac{\pi (2m+1)p}{2M} \right) \cos \left( \frac{\pi (2n+1)q}{2N} \right), \quad 0 \leq p, q \leq M, N-1 \]

\[ a_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ 1/\sqrt{2N}, & 1 \leq p \leq M-1 \\ 1/\sqrt{2M}, & 1 \leq q \leq N-1 \end{cases} \]

The DCT Inverse transform is given by:

\[ a_{p,q} = \frac{1}{M} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos \left( \frac{\pi (2m+1)p}{2M} \right) \cos \left( \frac{\pi (2n+1)q}{2N} \right), \quad 0 \leq p, q \leq M, N-1 \]

In general, watermarking scheme adopting the 8 × 8 block based DCT showed superiority to the whole image-based DCT in the sense of robustness except for the resizing. The block-based DCT transform divides image into non over lapping blocks and applies DCT to each block. An image divided into 8×8 blocks. Each of these 8 × 8 blocks of the original image is mapped to the frequency domain. This result in giving three frequency coefficient sets: low frequency sub-band, mid-frequency-sub-band and high frequency sub-band. DCT-based watermarking is based on two facts. The first fact is that much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image. The second fact is that high frequency components of the image are usually removed through compression and
noise attacks. The watermark is therefore embedded by modifying the coefficients of the middle frequency sub-band so that the visibility of the image will not be affected and the watermark will not be removed by compression.

VII. IMPLEMENTATION
The watermark Embedding described in details in the following steps:
Step 1) Read a image
Step 2) Take DCT of cover image. E.g. Let us take (8, 8) DCT.
Step 3) Place watermark into (5, 2) of each DCT block by comparing it with (4, 3) of same block in following way-
   If watermark is 0 then make (5, 2) greater.
   If watermark is 1 then make (5, 2) smaller.
Step4) Convert DCT domain to spatial domain image. This is watermarked image.
The watermark Extracting described in details in the following steps:
Step 1) Read a watermarked image
Step 2) Take DCT of watermarked image. E.g. Let us take (8,8) DCT.
Step 3) a) If (5, 2) of each DCT block is greater than 1, (4, 3) of same block, extract 0
   (b) If (5, 2) of each DCT block is lesser than (4, 3) of same block, extract 1.
Step 4) Convert DCT domain to spatial domain image. This is original image.

For testing the performance of DCT algorithm, the code is simulated with MATLAB software. The DCT Based watermarking algorithm is applied to number of input cover images and different Binary Watermarks. In this paper, 512 x512 Lena image and 50 x20 binary image is selected as the cover image i.e. original image and watermark image respectively.

The performance evaluation of this methods will be done by measuring their imperceptibility i.e. transparency and robustness. Here we use the normalized correlation (NC) to measure the similarity between original image and the watermarked image. Peak Signal-to-Noise Ratio (PSNR) measures the fidelity between the original image and the watermarked image. A larger PSNR indicates that the watermarked image more closely resembles the original image meaning that the watermarking method makes the watermark more imperceptible. Generally, if PSNR value is greater than 35dB the watermarked image is within acceptable degradation levels, i.e. the watermarked is almost invisible to human visual system.

VIII. CONCLUSION
This paper introduces a discrete cosine transform (DCT) digital watermark algorithm based on human vision characters. From this algorithm the nice peak signal to noise ratio is achieved which indicates watermarked image more closely resembles the original image and invisible for human eyes. Here conclusion is that the quantum of information embedded is determined by the specific application and directly effects on robustness of the system.

REFERENCES
7. I. Cox, J. Kilian, F. Leighton, and T. Shamoon,


