IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Discrete Cosine Transform-Based Copyright Security Of Digital Images

[1]Vivek Kumar Awasthi, [2]Mr. Mukhtar Ali

[1] M.Tech Scholar, [2] Assistant Professor

[1] Department of Computer Science & Engineering,

[1] Vishveshwarya Group of Institutions, Gautam Buddh Nagar, India

Abstract: Because imaging technology keeps advancing, we now need new options for guarding the copyrights of digital images. Copyright can be used to make sure an image and its ownership are recognized and to notice if an image is copied illegally. Nowadays, libraries are shifting because digital resources are more accessible and easier to use. In digital library settings, both pictures and writings are shared on the internet for scholars to study. At the same moment, care is given to preventing people from using the photos illegally for any commercial purpose.

We explain in this paper how perceptually based digital image watermarking uses the human eyes and brain to keep watermarks hidden. Any watermarking technique trying to add an invisible mark to an image can be considered perceptually based, no matter which other aspects it includes. Still, to ensure that watermarks are invisible and strong, advanced use of visual elements during the watermarking process has to be applied. We have offered a solution that increases the strength of the watermark..

Index Terms - Digital image watermarking, Spread-Spectrum techniques.

I. INTRODUCTION

INTRODUCTION

As the networked multimedia systems began to be used more, there was a need to ensure that the digital media is safeguarded more and more. The use of standards can be of great importance in protecting and implementing intellectual property rights. Digital media may be divided into text, audio, images, video, and software. Encryption, authentication, and time-stamping are some of the familiar ways to protect digital content.

A useful way to establish ownership of an image is to place a subtle signal in the media data itself. This is done by the use of digital watermarking that helps to retrieve ownership details even when the image has been manipulated.

The technology is an evolving field that borders on computer science, cryptography, signal processing, and communication disciplines. Digital watermarking [4, 5, 6] was invented as another mechanism that media professionals can use to secure their contents besides the conventional mechanisms that include Encryption and scrambling. Digital watermarking, like other emerging technologies [7, 8], is associated with several important concerns and questions.

- What exactly is identity?
- What methods are there for putting a digital watermark in a file and locating one later?
- Is it necessary to make the system stand up to a wide range of issues?
- What reasons exist for using digital watermarks, and at what times are they essential?
- What are the things watermarks might or might not be able to handle?
- How can digital watermarks be put to use?
- How can we decide if the technology is suitable for us?

- Are they practical, meaning, what extra protection do they give to content besides or in combination with the steps used in current copyright laws to handle grievances?
- Which opportunities exist in the business sector?
- What functions does digital watermarking have in content protection systems?

This paper aims to describe algorithms for checking the authenticity of images and stopping their forgery by watermarking them. Here is the block diagram that explains the watermarking process in digital images (Figure 1).

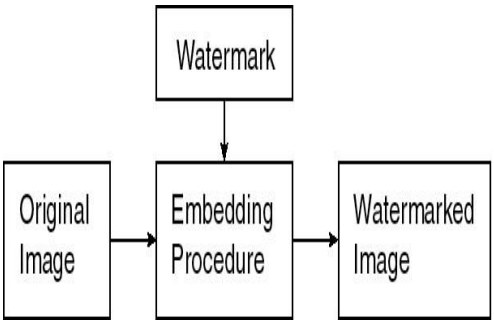


Figure 1: Block diagram of a watermarking algorithm

1.1 TYPES OF DIGITAL WATERMARKS

Watermarks and watermarking processes may be categorized rather widely. A single method is the incorporation of watermarks in the spatial domain. Otherwise, watermarking may be done in the frequency domain. It has been demonstrated that frequency domain methods are generally more robust than the traditional spatial domain approaches. The following picture illustrates what various kinds of watermarks look like.

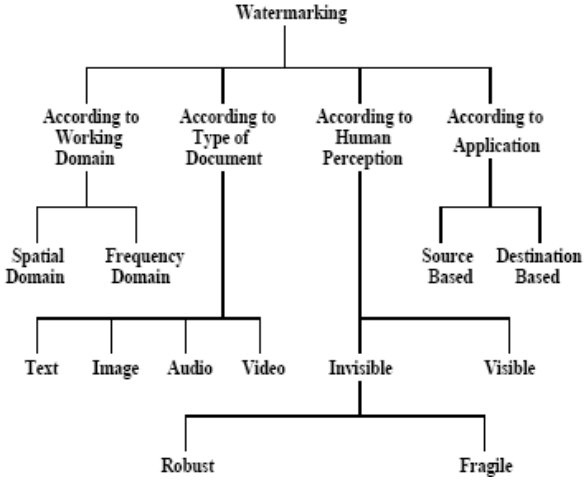


Figure 2: Types of watermarking techniques

Watermarking methods are mostly divided into four categories based on the kind of document used in them.

- Image Watermarking
- Video Watermarking
- Audio Watermarking
- Text Watermarking

According to people's perception, there are three primary kinds of digital watermarks.
Visible watermark

- Invisible-Robust watermark
- Invisible-Fragile watermark
- Dual watermark

The translucent watermark is put over the main picture as a secondary layer. You can only notice the watermark on a close look. Since invisible-robust watermarks are inserted without changing the pixels, it proves difficult to notice them and requires an appropriate process to reveal them. The invisible-fragile watermark is present in the image so that any changes to the picture would affect or get rid of the watermark. A dual watermark appears both as something you can see and something that is hidden [1]. An invisible watermark is used in addition to the visible one, as the example diagram shows.

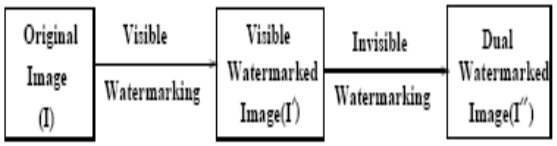


Figure 3: Schematic representation of dual watermarking

How a digital watermark is applied is stated below.

- founded on textual data.
- chosen by where the business is situated.

It is beneficial to use a watermark from the source for ownership so that all the copies of an image incorporate a unique mark that proves who the owner is. Using a source-based watermark makes it possible to notice changes to an image or any other electronic data. It's possible to use destination watermarking so that every copy given to a buyer is watermarked with their identifier. It is possible to use the destination-based watermark to find the buyer if someone attempts to sell the product unlawfully.

1.2 Application of Digital Watermarks

1.2.1 Visible Watermark

The following situations might call for using visible watermarks:

- Watermarks that can be seen to increase protection for your photos. When images are released on the Internet and the content owner sees the possibility of unauthorized commercial use (such as putting the images on coffee mugs), he/she may seek compensation for the use. Here, the customer wants a sign that makes the ownership visible, yet doesn't prevent the image from being used in special circumstances, such as study.
- Visible watermarks are put inside the images to signal who made them. Since images on the Internet are accessible, the owner wants to say that they manage and protect the original manuscripts, so viewers could step up and use their services.

1.2.2 Invisible Robust Watermark

In a series of situations, invisible robust watermarks prove to be beneficial.

- Technologies to mark images with hidden features to find any unauthorized use. In this case, the Digital imagemaker is afraid that someone might buy his images and distribute them for free, so the owner will not get any licensing income.
- Invisible watermarking is mostly applied in determining ownership of digital content. To give an example, when a seller of digital images suspects that one of their images has been used without the due payment of royalties, then the invisible watermark that is embedded in the image can be used as evidence that the image is theirs.

1.2.3 Invisible Fragile Watermarks

Let's now highlight the uses of invisible, fragile watermarks.

- A trustworthy camera that uses hidden watermarking for its pictures. In this situation, images are taken with a digital camera that will be used later in news reports. The goal of a news agency here is to confirm that the picture shown is exactly as captured without the change of important details. With this, during image capture, an invisible watermark is added so that when the image is published, its presence proves it has not been reviewed after being captured.

- Using invisible watermarks to find when an image stored in a digital library is altered. In this situation, digital libraries have been made with images like fingerprints, but the content owner doesn't want to check each new image against the existing scanned ones, since any alteration needs to be identified automatically.

2CURRENT STATE OF THE ART

When watermarking a multimedia file, data in the form of a watermark or signature is inserted, and later, anyone can find the watermark by searching the file to state its authenticity. The object can be an image, sound, or video recording. Digital watermarks are easy to illustrate by placing a clear "seal" above a picture to indicate the copyright. However, the watermark could display the purchaser's details as well as other information.
On the whole, any watermarking scheme (algorithm) is made up of three important pieces.

- The watermark is the emblem of each country.
- The encoder is what you call the insertion algorithm.
- The components relating to decoding and comparing (verification or extraction, or detection algorithms).

Every owner's watermark is different and can be used differently, depending on the object; the watermark gets mixed into each object by the marking code. This algorithm identifies the owner and also confirms that the object is safe from any tampering.

2.1 Embedding Process

Where I is the original image and S = {s 1, s 2, ...} is the signature. The watermarked image thus obtained is denoted by $\hat{I}$.
The encoder E, using the original image I and the signature S, produces the new watermarked image $\hat{I}$.

$$E(I, S) = \hat{I} \quad (1)$$

It is important to say that the signature S may vary with image I. Encoding still takes place as explained by Eqn.1 in such situations. The next figure represents how encoding is carried out.

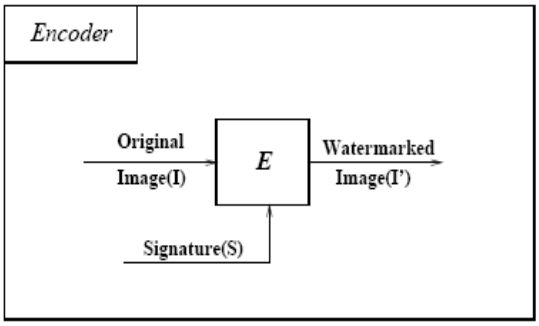


Figure 4: Encoder

2.2 Extraction Process

The decoder D is given a picture J (this image may be watermarked or different in some way) and brings out a unique signature S' contained in the image. At this stage, I can have an extra picture I can have, representing the clean non-watermarked image of J. This happens because some watermarks utilize the original images to enhance their ability to resist any change to the image. Mathematically,

$$D(J, I) = S' \quad (2)$$

The signature S' prime so extracted is compared with the signature sequence of the original owner under a comparator function C_δ. The result of this process is binary: 1 means the existence of a match, 0 means no match.

$$C_\delta(S', S) = \begin{cases} 1, & c \le \delta \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

The correlator is represented by C; the correlation of the two signatures is c; and the threshold point is represented by δ. In most cases, a watermarking scheme is understood as a three-tuple (E, D). The next figures illustrate the decoder and the comparator explained above.

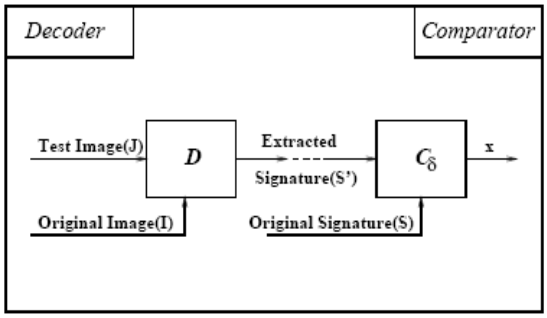


Figure 5: Decoder

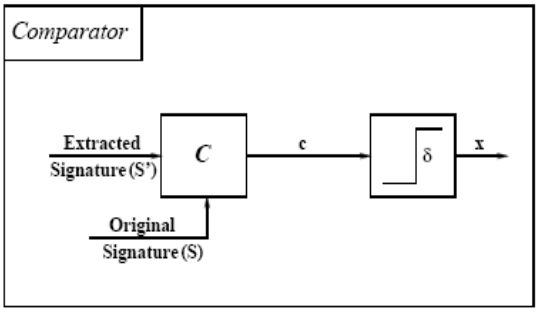


Figure 6: comparator

An effective watermark ought to be detectable or extractable. The method employed depends upon the way watermark is embedded and the particular algorithm utilized. In some watermarking schemes, the embedded watermark may be extracted in its original form (this is called watermark extraction). In other schemes, the system merely verifies the existence of specific watermark signal in the image, and this process is called watermark detection. It is worth mentioning that extraction may be used as evidence of ownership whereas detection can only be used to affirm ownership.

2.3 A spread spectrum watermark embedded in the DCT domain

The idea of spread spectrum communications is used in the frequency domain digital watermarking method mentioned in [2]. The motivation behind the technique comes from making the watermark clear and making it hard to erase. It is obvious from the reported results that the technique achieves high transparency, handles signal processing well, and makes it hard to remove the watermark. The same technique is not affected by cropping, extremely reduced quality JPEG compression, printing and rescanning, and collusion with a set of images protected by watermarks. It was realized here that a watermark placed in the image's visually significant part offers better security.

W is composed of zero-mean unit-variance, normally distributed samples. The DCT operates on every part of the image, and low-frequency components, along with W (except for the DC component), are placed at wanted locations. Take X as the initial image, Y as the image with the watermark, X_D and Y_D as the DCT coefficients of X and Y, respectively. The coefficients can be reorganized in the same manner as done in JPEG's zigzag pattern. $X_D(i)$ is the i^{th} DCT coefficient in X_D, and $Y_D(i)$ means the same for the Y_D. W(i) means the i^{th} bit in the watermark, and a is the scale factor that keeps $Y_D(i)$ from taking unsuitable values. At this point, the marks needed are applied.

$$Y_D(i) = X_D(i)(1 + aW) \quad (4)$$

W can be introduced to X_D by using the alternative equations listed in [2]. In the last step, Y_D is inversely transformed into Y to finish the marking step. As shown in Figure 7 on the upper left, I used numbers = 0.1, 0.5, and 1.0 to mark where the wave is higher. According to the authors, a should be assigned a value of 0.1 through a statistical study.

The first thing to do in verification is to copy the wavelet transform W from the possibly forged image Z. Z_D stands for Z's vector of DCT coefficients. W* is derived by using the operations explained by W.

$$W^*(i) = \frac{1}{a}\left[\frac{Z_D(i)}{X_D(i)} - 1\right] \quad (5)$$

The degree of similarity between W* and W is found by carrying out the procedure given below.

$$S(W, W^*) = \frac{W \cdot W^*}{\sqrt{W^* \cdot W^*}} \quad (6)$$

If W is not used to stamp the image, S is assigned the value of zero. If W* and W have just a small difference (i.e., W is present in Z, although slightly changed), then E[S] >> 0. The hypothesis test on S finds out whether object W exists within the image. It allows for many watermarks and is much more secure against different kinds of attacks than the spatial methods.

The algorithm was among the first to try to make watermark embedding respond to different images. It is because the strength of a watermark relies on the intensity of the DCT values in the original image. Thus, the signal of the watermark is more prominent in DCT values that have large intensities, and it gets much weaker in places with small DCT intensities. Generally, the added watermark signal can't be removed and is visible through most pictures. Besides, as the DCT transform is done over the entire picture rather than the usual blocks used in other compression schemes, the strategy does not control where the watermark is buried. To put it simply, including a watermark value in one DCT coefficient changes all aspects of the image; it is not possible to control this change at the local level in this framework. To reach the optimal DCT weighting, the framework could use a perceptual model, but it has to be revised so that the watermark adapts better to the image and its viewers.

Figure 7: Example of DCT-spread spectrum technique

Another method that is used globally tones down DCT coefficients by using a single-dimensional binary sequence with values that are positive or negative [3]. The DCT of the original image is processed first. During marking, the DCT coefficients are grouped by how large their magnitude is. After that, the owner sets a specific percentage for P and determines the biggest n coefficients that contribute P percent to the total energy.

Watermarks are then put on all of the coefficients that appear in the AC coefficients list. When $X_D(i)$ is chosen as a selected coefficient

$$Y_D(i) = X_D(i) + W(i) \quad (7)$$

A greater value of P allows W to be placed in X more often, yet raises the possibility that W becomes noticeable. Both W* and the list of selected coefficients have to be kept secret. Initially, it removes W from the collection of coefficients ZD has labeled.

$$W^*(i) = Z_D(i) - X_D(i) \quad (8)$$

After that, a method similar to [2] can be used to verify W*. We should note that an X in [2] and [3] is needed to pull out the watermark.

3PROPOSED WORK

For the protection of images online, visible watermarking is a kind of digital watermarking used most. I have explained visible watermarking techniques that work in the DCT domain in this paper. For this reason, a mathematical model has been put together. The authors have suggested an algorithm in the DCT domain to help the watermark stand up to changes.
The steps I used to carry out this task are the following:

- At the beginning, digital watermarking for images that make the highest quality is introduced and discussed.
- The next step is to use the tool (MATLAB) to put the watermark into the original image in the DCT domain.
- After that, the process of extracting the watermark will take place. The comparison of the watermark before and after extraction is also shown.
- Here, it is also important to assess the quality of images.

3.1 *Implementation of Work*

We suggested using a DCT-based algorithm as mentioned in section 2.3, and the main change is that we focus on adding a random PN-sequence to the center parts of each DCT block. This results in a watermark that is tough to remove and useful even with most types of images. The steps to embed watermarks in this approach are given below.

- Determine the value of the gain factor (K) for the embedder.
- Choose the size of the DCT blocks you want to use.
- Run a search to choose sequences that are less connected with each other (T, F).
- Outlines the middle range of frequencies that are processed by an 8x8 DCT.
- Figure out the size of the first image.
- Pick the size you want for the watermark image.
- Transform the message to a vector format.
- Make the message as long as possible by putting 1's at the end, if needed.
- Put together the new watermarked image.
- Generate code sequences for the two states "1" and "0
- Work on the image's data in sections rather than looking at it all at once.
- Use the DCT to change the block values.
- If the bit in the message is a zero, then insert the PN-sequence-zero into the center parts of the DCT-block.
- If this isn't possible, add PN-sequence-one to the mid-band parts of the DCT-block.
- Go back from the transform domain to the spatial domain.
- Go on to the next part of the road. Keep going down each row so that you finish the board.
- Make the watermarked image into a uint8 and save it as a file.
- Show when the request is processed and the result is given.

- Feature an image that has “watermarks” on it.

3.2 *Experimental Analysis and Results*

The results provided below demonstrate the effectiveness and performance of our digital watermarking method in embedding and extracting water mark image into the original digital image in the DCT (Discrete Cosine Transform) domain.
The picture named “Lena,” which is a grayscale image that is 512 pixels square, has been used for the test, as indicated in Figure 8. We take the grayscale image “Dmg-1” as the watermark image, and you can see it in Figure 9. As you can see, the watermarked image is demonstrated in Figure 10.

Figure 8: Original image of Lena

Figure 9: Watermark image

Figure 10: Watermarked image of Lena

We checked the quality of each image by using peak signal-to-noise rate (PSNR). The equation for PSNR is the following:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)\text{dB}. \quad (9)$$

To put it another way, H × W MSE is calculated for an image of these dimensions.

$$MSE = \frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(o_{ij} - \tilde{o}_{ij})^2, \quad (10)$$

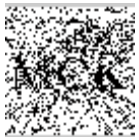
Where O_{ij} is the original pixel value and $\tilde{O}_{ij}$ is the resultant pixel value after processing. Also, the effectiveness of the copyright protection system in resisting a particular form of attack is determined with the help of the Accuracy Rate (AR). The AR calculates the ratio of the correct predictions and the total number of predictions made.

$$AR = \frac{CP}{NP}, \quad (11)$$

Where NP is the total number of pixels in the watermark image, and CP is the number of correctly detected pixels in the watermark image extracted after modifying or attacking the image.

The experimental results are depicted in Figure 11, where it can be seen how the watermarked image and the extracted watermark look when the gain factor K varies.
Table 1 illustrates numerous observations made in the course of the experiment.
.

1. K=10

2. K=20


3. K=40


4. K=50


5. K=70


Figure 11: (i) Watermarked image,
(ii) extracted watermark image

Table 1
The quality rates under various executions

Gain Factor (K)	Execution Time	Accuracy Rate	Peak-Signal to noise rate (PSNR)
K= 10	2.7344	78.1250	53.8851
K= 20	2.7656	85.9375	55.5562
K= 40	2.7969	98.4375	58.4224
K=50	2.7500	98.4375	59.2029
K=70	2.7813	100	84.2544

4CONCLUSIONS

We have outlined how image digital watermarking is now being performed with techniques that do not show visually and work on how humans process images. Most of these approaches depend on either being very transparent or working at particular high-frequency ranges to keep the marks out of view. Watermarks that are adapted to images make use of visual techniques to boost the visible strength of the watermark but keep it inconspicuous. This kind of algorithm was more likely to remain safe during different attacks that used both linear and nonlinear signal processing. The main thing that distinguishes the digital world from the past is the need to protect intellectual property rights. The techniques described in this paper won't work perfectly, but they can assist in proving the claims of ownership needed for intellectual property law enforcement.

REFERENCES

[1] S.P. Mohanty, et al., "A Dual Watermarking Technique for Images", *Proc. 7th ACM International Multimedia Conference, ACM-MM'99*, Part 2, pp. 49-51, Orlando, USA, Oct. 1999.

[2] I. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, December, 1997, pp. 1673-1687.

[3] F. M. Boland, J. J. K. Ó Ruanaidh and C. Dautzenberg, "Watermarking digital images for copyright protection," *Proceedings of the International Conference on Image Processing and its Applications*, Edinburgh, Scotland, July 1995, pp. 321-326.

[4] R. B. Wolfgang and E. J. Delp, "Overview of image security techniques with applications in multimedia systems," *Proceedings of the SPIE International Conference on Multimedia Networks: Security, Displays, Terminals, and Gateways*, November 4-5, 1997, Dallas, Texas, vol. 3228, pp. 297-308.

[5] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data embedding and watermarking technologies," to appear in *Proceedings of the IEEE*, 1998.

[6] I. J. Cox and M. L. Miller, "A review of watermarking and the importance of perceptual modeling," *Proceedings of the*