International Journal of Recent Trends in Engineering Vol. 1, No. 2, May 2009

Digital Watermarking using Image Fusion Method

Prof. S. C. Tamane, Dr. R. R. Manza and Dr. R. R. Deshmukh,
MGM's, Jawaharlal Nehru Engineering College, IT Department, Aurangabad, India,
sharvaree73@yahoo.com
Dr. Babasaheb Ambedkar Marathwada University, Computer Department, Aurangabad, India
ratnadeep_deshmukh@yahoo.co.in, ramesh_manza@yahoo.com

***Abstract*-- With the growing popularity of digital Medias through the WWW, intellectual property needs copyright protection, prevention of illegal copying and verification of content integrity. The new data hiding techniques need to be developed that satisfy the requirements of imperceptibility, robustness, capacity, or data hiding rate and security of the hidden data in order to keep the distribution of digital multimedia work both profitable for the document owner and reliable for the customer.**

Previous research [01] indicates that significant portions of the host image, e.g. the low frequency components, have to be modified in order to embed the information in a reliable and robust way. This led to the development of watermarking schemes embedding in the frequency domain. The wavelet transform has the number of advantages over other transforms such as the DCT that can be exploited for both, image compression and watermarking applications. Therefore it is imperative to consider the wavelet transform domain for watermarking applications.

Key words: **Digital Watermarking, Wavelet Transform, Robustness, Image Fusion.**

I. INTRODUCTION

A digital watermark can be described as a visible or preferably invisible identification code that is permanently embedded in the data. It means that it remains present within the data after any decryption process. A general definition can be given as: "Hiding of a secret message or information within an ordinary message and the extraction of it at its destination". Complementary to encryption, it allows some protection of the data after decryption. The goal is to embed some information in the image without affecting its visual content. In the copyright protection context, watermarking is used to add a key in the multimedia data that authenticates the legal copyright holder and that cannot be manipulated or removed without impairing the data in a way that removes any commercial value. Figure1 shows a general watermarking scheme in order to give an idea of the different operations involved in the process.

The first distinction that one needs to do in the study of watermarking for digital images is the notion of visible watermarks *versus* invisible ones. The first ones are used to mark, obviously in a clearly detectable way, a digital image in order to give a general idea of what it looks like

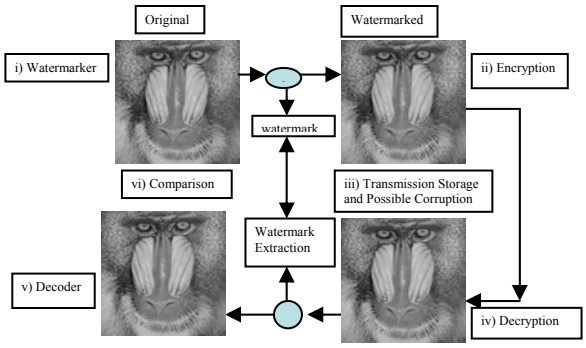


Figure1: General Watermarking Scheme

while preventing any commercial use of that particular image. The purpose here is to forbid any unauthorized use of an image by adding an obvious identification key, which removes the image's commercial value. On the other hand, invisible watermarks are used for content and/or author identification in order to be able to determine the origin of an image. They can also be used in unauthorized image's copies detection either to prove ownership or to identify a customer. The invisible scheme does not intend to forbid any access to an image but its purpose is to be able to tell if a specified image has been used without the owner's formal consent or if the image has been altered in any way. It is possible to differentiate two ways of embedding Multi-resolution Watermarking for Digital Images:

The first watermarking scheme that was introduced works directly in the spatial domain. By some image analysis operations (e.g. Edge detection), it is possible to get perceptual information about the image, which is then used to embed a watermarking key, directly in the intensity values of predetermined regions of the image

Another way to produce high quality watermarked image is by first transforming the original image into the frequency domain by the use of Fourier, Discrete Cosine or Wavelet transforms for example. With this technique, the marks are not added to the intensities of the image but to the values of its transform coefficients. Then inverse transforming the marked coefficients forms the watermarked image. The use of frequency based transforms allows the direct understanding of the content of the image; therefore, characteristics of the human

visual system (HVS) can be taken into account more easily when it is time to decide the intensity and position of the watermarks to be applied to a given image.

II. Application Areas

Digital watermarking is considered as an imperceptible, robust and secure communication of data related to the host signal, which includes embedding into and extraction from the host signal. For copy protection applications, the watermark must be recoverable even when the watermarked signal undergoes a considerable level of distortion, while for tamper assessment applications, the watermark must effectively characterize the modification that took place. Some applications of invisible watermarks are listed here: Fingerprinting, Indexing, Copyright Protection & Owner Identification, Broadcast Monitoring, Copy Protection, Data Authentication, Data Hiding (Covert Communications), Medical Safeties. From the applications mentioned above, one can divide watermarks into two distinct types: Robust, for the first five applications and Fragile for the last three.

III. Wavelet Transform

Mathematical transformations are applied to signals to obtain further information from that signal that is not readily available in the raw signal. For time domain signal, the time amplitude representation is not always the best representation of the signal for most signal processing related applications. The same is true for two-dimensional image. The pixel or space domain representation is not always the best representation

In many cases the most distinguished information is hidden in the frequency content of the signal. The frequency spectrum of a signal is basically the frequency components (spectral components) of that signal i.e. it shows what frequencies exist in the signal. With the help of Fourier Transform we can measure frequency, or find the frequency content of a signal. FT is a reversible transform, i.e. it allows going back and forward between the raw and processed (transformed) signals but, only either of them is available at any given space (time). When the space localization of the spectral components is needed, a transform giving the good space (time)-frequency representation of the signal is needed and for this one has to go for many of the following transform: Short Time Frequency Transform (STFT) and Wavelet transform (CWT and DWT).

The Discrete wavelet transform has three properties that make it difficult to use directly in the continuous form. The 1st is the redundancy of the CWT. In CWT, the wavelet transform is calculated by continuously shifting a continuously scalable function over a signal and calculating the correlation between the two. These scaled functions will be nowhere an orthogonal basis and obtained wavelet coefficients will therefore be highly redundant. For most practical cases this redundancy has to be removed.

IV. Proposed Watermarking Technique

Image watermarking imperceptibly embeds data into a host image [5]. The general process of image watermarking is depicted in figure2. The original image (host image) is modified using the signature data to create the watermarked image. In this process some error or distortion is introduced. To ensure transparency of the embedded data, the amount of image distortion due to the watermark embedding process has to be small. The watermarked image is then distributed and may circulate from legitimate to illegitimate customers. Thereby, it is subjected to various kinds of image distortion. The successive stages of the watermarking processes defined in the figure2 are: The embedding stage (figure 3), the distribution stage (figure 4), the extraction stage (figure 5), and the decision stage.

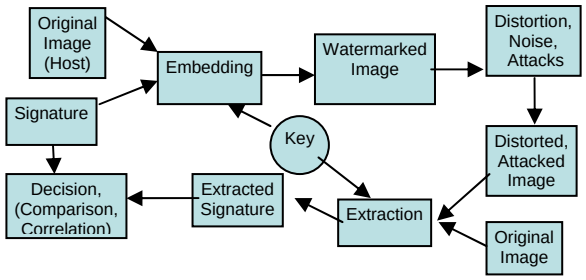


Figure2: The Data Hiding Model, a General Overview

A. The Embedding Stage

The host image is first transformed to a domain that facilitates data embedding. This work exclusively considers the wavelet and wavelet packet transform domains. The signature data can be some binary data or a small image (a logo). Typically the signature data has to be encrypted to de-correlate the information and subjected to some error-correcting coding scheme.

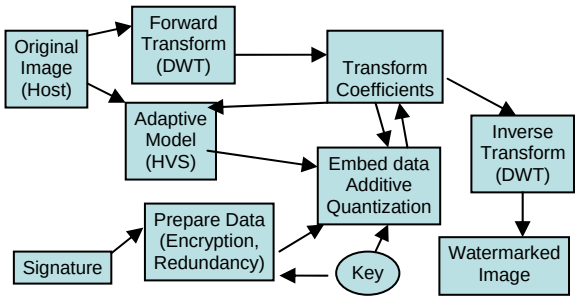


Figure 3: Model of the Watermark Embedding Stage

Next, the subset of the transform coefficients is modified with the prepared signature data. By choosing a suitable frequency transform domain and selecting only certain coefficients, a lot of HVS modeling can be done implicitly. Finally, the inverse transformation is applied on the transform domain coefficients to produce the watermarked image.

B. Distribution

The watermarked image is then distributed, or published on a web server or sold to a customer. During transmission and distribution of watermarked image, not

only compression adds distortion to the host data, but also transmission errors and common image processing tasks, such as contrast enhancements, re-sampling and gamma correction, contribute errors to the watermarked image. All manipulation of the watermarked image data has to be seen as an attack on the embedded information. Modifications that occur during normal image processing are called as coincidental attack. The attacks that attempt to weaken, remove or alter the watermark itself are termed hostile or intentional attacks.

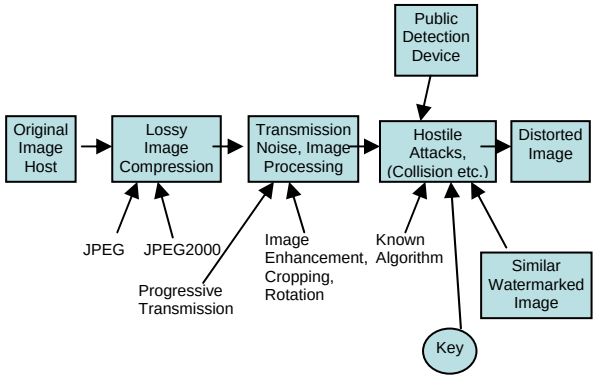


Figure4: Model of the Distribution of the Watermarked Image

C. Extraction Stage

Eventually, after the watermarked image has undergone severe distortion, one would like to extract the embedded signature from the host data this can be done by the party that embedded the watermark, the customer that received the image, a designated party- such as a web crawler that scan the internet for illegal copies of the protected work or a legal prosecution official- or by a third party. In the first case, the secret key used to embed the watermark as well as the original image might be available. We call detection systems that have access to the secret (private) key and original image non-oblivious, non-blind or private watermarking systems.

The other extreme is the case where neither the private key nor the original image is available during the extraction process. These watermarking systems are called public key watermarking systems.

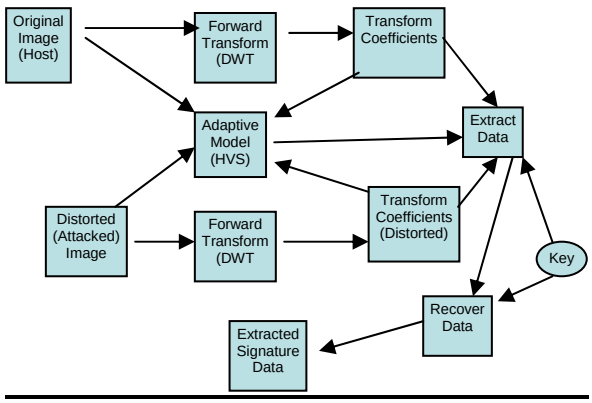


Figure5: Model of the watermark extraction stage

D. Decision Stage

In the decision stage, the watermarking system analyzes the extracted data, depending on the type of the application and the nature of the signature data, the decision stage can produce a number of different outputs.

For image copy protection applications, the output of the watermarking system can range from simple to more complicated answers. In the simplest case, the result is just a yes/no decision indicating if the copyright holder's mark has been found in the received image data. More complex systems return the embedded logo image or the textual copyright information that was placed into the host image data. A widely used similarity measure between the original watermark and the extracted watermark sequence is the normalized correlation for pseudo random sequences δ.

The extracted watermark yes/no answer can be derived from the similarity measure δ with an appropriate threshold τ, i.e. if $\delta >= \tau$ then is watermark is detected otherwise watermark could not be found in the image.

Image labeling and data hiding applications will typically try return the message originally embedded. Since message corruption can not be tolerated, the use of error correcting codes is mandatory for this type of application.

V. WATERMARKING ALGORITHM

A. Image Fusion Algorithm

Watermarking algorithms which embed meaningful data in the form of a logo image instead of a pseudo-random number sequence are called image-fusion watermarking algorithms. The logo image is generally smaller than the host image. Before being added to the host signal, the logo image is encrypted (de-correlated) and suitably transformed.

There are two important advantages of embedding a logo image as watermark data. First, the extracted image can be correlated with the originally embedded image by a human observer, building on the superior pattern-matching capabilities of the human brain. Second the existence of a visual logo in the questionable image might be much better proof of ownership than a high statistical correlation value.

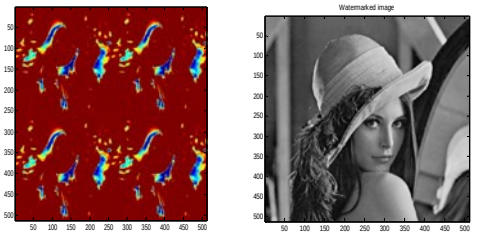
Watermark: The Watermark is a gray scale image, with as least 25% of the host image size. **Decomposition:** The algorithm proposes using 2-level decomposition on both, the host and the logo image, with the Haar wavelet filter. The wavelet domain representation of the host image is denoted by f(m,n), the DWT coefficients of the logo image by w(m,n). **Coefficient selection:** Each approximation coefficient of the host image whose value is greater than threshold value (i.e. 250) is modified to embed the logo image. **Embedding:** The host and logo image coefficients of each subband are linearly scaled. Since the logo image is smaller than the host image, the coefficients have to be expanded. After adding the expanded logo image to a scaled version of the host image, image representation is

scaled back using the original minimal and maximal coefficients values per subband. Finally the fused (combined) image is produced via the IDWT. **Extraction:** The extracted watermark sequence is compared to the originally embedded watermark using the normalized correlation of the sequences as a similarity measure δ. The similarity measure δ varies in the interval [-1, 1], a value above 0 and close to 1 indicates the extracted sequence matching the embedded sequence and therefore we can conclude that the image has been watermarked. **Discussion:** The proposed method allows hiding surprisingly high amounts of image data in a host image. The current implementation is limited to logo images that are a quarter of the size of the host image. However this constraint can easily be removed by exploiting the multiresolution property of the wavelet transform and performing more decomposition steps.

VI. Results

A. Original Image and B. Watermark resp.

C. Transformed Watermark Image. And D. Watermarked Image resp.



VII. Conclusion & Future Scope

In this paper, a novel algorithm for image watermarking has been presented.

The algorithm embeds the watermark code by modifying the DWT coefficients 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 DWT 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, DWT 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

[1] Ingemar J. Cox,Joe Kilian, Tom Leighton, Talal G. Shamoon on "Secure Spread Spectrum Watermarking from Multimedia, IEEE, ICIP' 97, volume 6, Pages 1673-1687, Santa Barbara, California, USA, October 1997.

[2] Maryline Charrier, Diego Santa Cruz, and Mathias Larsson, JPEG2000, the Next Millennium Compression Standard for Still Images. In Proceedings of the IEEE, ICMCS '99volume 1, pages 131,132, Florence Italy, June 1999

[3] Mahalingam Ramkumar, Ali N. Akansu, and A. Aydın Alatan. A robust data hiding scheme for images using DFT. In Proceedings of the 6th IEEE International Conference on Image Processing, ICIP' 99,pages 211-215, Kobe, Japan, October 1999 .

[4] Improved Wavelet-Based Watermarking Through Pixel-Wise Masking Mauro Barni, Member, IEEE, Franco Bartolini, Member, IEEE, and Alessandro Piva, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 5, MAY 2001

[5] Digital Image Watermarking in the wavelet transform domain, Diplomarbeit, Peter Meerwald, Salzburg,am , 11 Janner 2001.

[6] A. G. Bors, "Watermarking Mesh-Based Representations of 3-D Objects Using Local Moments," IEEE Trans. on Image Processing, vol 15, no. 3, pp. 687- 701, Mar. 2006. © IEEE