A SURVEY ON DIGITAL WATERMARKING APPROACH BASED ON INTEGER WAVELET TRANSFORM

BODDULA MADHAVI 1 DR. RAJKUMAR L BIRADAR2 DR. K. RAMA LINGA REDDY3
Department of ETM1 Associate professor 2 H.O.D. (ETM)3
G. Narayanamma Institute of Technology and Science (For Women), Hyderabad, INDIA

Abstract

The prominence of digital image processing domain has been increased from last few decades due to its advanced research areas such as medicine, biometrics, military, robotics etc. In this work an important issue has taken as area of research i.e. protecting the privacy information from the unauthenticated users either as accidental or incidental ways. Although tremendous progress has been made in the past years but still protecting the privacy information is concerned area in the field of security. A novel image authentication scheme for gray scale images are implemented in this work and the process of the embedding digital watermark is carried by performing the quantization process on the image. The novel things implemented in the proposed work is detection of tampered parts of the image and to detect minute modification of an image and to embed the watermark mid frequency band of a second level DWT transform was used. An approximation of the original image based on LL band was stored as a recovery mark for restoration of the image. Watermarked image has achieved a good PSNR value of 40 dB compared to original cover image. Restored image quality was also very good with a PSNR of more than 35 dB compared to unmodified watermarked image even when 25% of the received image is cropped. Finally the simulation results reveals that the proposed method provides the reliable balance between fidelity of the watermarked image and the quality of the restored image

KEYWORDS: Authentication, Tampered part detection, Privacy protection, Image restoration, IWT

Literature review 1

A Dual Watermarking Technique for Images

Saraju P.Mohanty, K.R. Ramakrishnan, Mohan Kankanhalli

Digital watermarking is the technique in which a visible/invisible signal (watermark) is embedded in a multimedia document for copyright protection. In this paper, we propose a watermarking scheme called “dual watermarking”. Dual watermark is a combination of a visible watermark and an invisible watermark.

Digital watermarking is defined as a process of embedding data (watermark) into a multimedia object to help to protect the owner’s right to that object. The embedded data (watermark) may be either visible or invisible. In visible watermarking of images, a secondary image (the watermark) is embedded in a primary image such that watermark is intentionally perceptible to a human observer whereas in the case of invisible watermarking the embedded data is not perceptible, but may be extracted by a computer program.
Some of the desired characteristics of watermark. It is difficult to develop a visible watermarking algorithm that satisfies all the characteristics listed in [1, 2] and that works effectively for all types of images. Moreover, a visible watermark howsoever robust it may be can always be tampered using various software.

To detect such kind of tampering (in worst case to protect the image when the visible watermark is fully removed) an invisible watermark can be used as a backup. In this paper, we propose a watermarking technique called dual watermarking. The dual watermark is a combination of a visible watermark and an invisible watermark. We first insert the visible watermark in the original image and then an invisible watermark is added to the already visible-watermarked image. The final watermarked image is the dual watermarked image.

We have presented a watermarking technique called dual watermarking technique. The dual watermark is a combination of visible and an invisible watermark. The dual watermark serves two ways first, it establishes the owner’s right to the image and second, it detects the intentional and unintentional tampering of the image. The watermarking technique works for both gray and color images. For the color image the watermark is put in the Y-component. The watermark can find applications in digital library.

**Literature review 2**

**Secure Spread Spectrum Watermarking for Multimedia**

Ingemar J. Cox, Senior Member, IEEE, Joe Kilian, F. Thomson Leighton, and Talal Shamoon

This paper presents a secure (tamper-resistant) algorithm for watermarking images, and a methodology for digital watermarking that may be generalized to audio, video, and multimedia data. We advocate that a watermark should be constructed as an independent and identically distributed (i.i.d.) Gaussian random vector that is imperceptibly inserted in a spread-spectrum-like fashion into the perceptually most significant spectral components of the data. We argue that insertion of a watermark under this regime makes the watermark robust to signal processing operations (such as lossy compression, filtering, digital-analog and analog-digital conversion, requantization, etc.), and common geometric transformations (such as cropping, scaling, translation, and rotation) provided that the original image is available and that it can be successfully registered against the transformed watermarked image. In these cases, the watermark detector unambiguously identifies the owner. Further, the use of Gaussian noise, ensures strong resilience to multiple-document, or collusional, attacks. Experimental results are provided to support these claims, along with an exposition of pending open problems.

A need for electronic watermarking is developing as electronic distribution of copyright material becomes more prevalent. Above, we outlined the necessary characteristics of such a watermark. These are: fidelity preservation, robustness to common signal and geometric processing operations, robustness to attack, and applicability to audio, image and video data.

**Literature review 3**

**Watermarking Digital Images for Copyright Protection**
J.J.K. O Ruanaidh, W.J. Dowling, F.M. Boland

A watermark is an invisible mark placed on an image that can be detected when the image is compared with the original. This mark is designed to identify both the source of an image as well as its intended recipient. The aims of this paper are to present an overview of watermarking techniques and to demonstrate a solution to one of the key problems in image watermarking, namely how to hide robust in visible labels inside grey scale or color digital images.

This paper has outlined a scheme for embedding robust watermarks in digital images. The watermarks are designed to be visible, even to a careful observer, but contain sufficient information to identify both the origin and intended recipient of an image with a very low probability of error. One key feature of the transform based methods is that information bits can be placed adaptively, thereby making the watermark more robust to attack. A watermark is made imperceptible because it is designed to match

Literature review 4

Overview of image security techniques with applications in multimedia systems

Raymond B. Wolfgang and Edward J. Delp

The growth of networked multimedia systems has created a need for the copyright protection of digital images and video. Copyright protection involves the authentication of image content and/or ownership. This can be used to identify illegal copies of a (possibly forged) image. One approach is to mark an image by adding an invisible structure known as a digital watermark to the image. Techniques of incorporating such a watermark into digital images include spatial-domain techniques, transform-domain algorithms and sub-band filtering approaches.

The recent growth of networked multimedia systems has increased the need for the protection of digital media. This is particularly important for the protection and enforcement of intellectual property rights. Digital media includes text, digital audio, images, video and software. Many approaches are available for protecting digital data; these include encryption, authentication and time stamping. In this paper we present algorithms for image authentication and forgery prevention known as watermarks. Figure 1 shows the block diagram for watermarking digital images.

We have overviewed many of the recent techniques in the digital watermarking of images. Other important topics include the protection of documents, audio and video. While all of the techniques are not foolproof, it is important that they help preserve the “chain of evidence of ownership” that is consistent with intellectual property law.

Literature review 5

Multimedia Data-Embedding and Watermarking Technologies

MITCHELL D. SWANSON, MEMBER, IEEE, MEI KOBAYASHI, AND AHMED H. TEFWI

In this paper, we review recent developments in transparent data embedding and watermarking for audio, image, and video. Data-embedding and watermarking algorithms embed text, binary streams, audio, image, or video in a host audio, image, or video signal. The embedded data are perceptually inaudible or invisible to maintain the quality of the
source data. The embedded data can add features to the host multimedia signal, e.g., multilingual soundtracks in a movie, or provide copyright protection. We discuss the reliability of data-embedding procedures and their ability to deliver new services such as viewing a movie in a given rated version from a single multicast stream. We also discuss the issues and problems associated with copy and copyright protections and assess the viability of current watermarking algorithms as a means for protecting copyrighted data.

The past few years have seen an explosion in the use of digital media. Industry is making significant investments to deliver digital audio, image, and video information to consumers and customers. A new infrastructure of digital audio, image, and video recorders and players, on-line services, and electronic commerce is rapidly being deployed. At the same time, major corporations are converting their audio, image, and video archives to an electronic form.

Digital media offer several distinct advantages over analog media: the quality of digital audio, image, and video signals is higher than that of their analog counterparts. Editing is easy because one can access the exact discrete locations that should be changed. Copying is simple with no loss of fidelity. A copy of a digital media is identical to the original. Digital audio, image, and videos are easily transmitted over networked information systems.

**Literature review 5**

*A review of watermarking and the importance of perceptual modeling*

*Ingemar J. Co x and Matt L. Miller*

A watermark embeds an imperceptible signal in to data such as audio, video and images, for a variety of purposes, including captioning and copyright control. In this paper, we first outline the desirable characteristics of digital watermarks. Previous work in digital watermarking is then reviewed. Early work identified redundant properties of an image (or its encoding) that can be used to encode watermarking information. The early emphasis was on hiding data, since the envisioned applications were not concerned with signal distortions or intentional tampering that might remove a watermark. However, as watermarks are increasingly used for purposes of copy right control, robustness to common signal transformations and resistance to tampering have become important considerations. Researchers have recently recognized the importance of perceptual modeling and the need to embed a signal in perceptually significant regions of an image, especially if the watermark is to survive lossy compression. However, this requirement with the need for the watermark to be imperceptible, several recent approaches that address these issues are discussed.

**Literature review 6**

*Digital watermarking for digital images using wavelet transform*

*Yusnita Yusof Othman O. Khalifa*

The field of digital watermarking has recently seen vast interests covering theoretical studies, novel techniques, attacks and analysis. This is due to the fact that over the last 15 years, the watermarking community has focused on developing and introducing new techniques for watermark
embedding and detection. Analysis of these techniques leads to methods for attack and development of countermeasures which then used to discover faults and limitations in applications, encouraging the development of better ones. In this paper, comprehensive overview of digital watermarking are discussed. This includes the general model, types, applications and future trends of current implementations. The proposed technique is described and analyzed. The paper concludes with future plans of the chosen method in digital watermarking.