A Quick Glance over the Digital Watermarking

Priyanka Patel¹ Priyanka Trikha²
¹M. Tech. ²Assistant Professor, Computer Science and Engineering Department
¹,²Sri Balaji College of Engineering & Technology, Jaipur

Abstract— Digital watermarking is a process for modifying physical or electronic media to embed a machine-readable code into the media. The media may be modified such that the embedded code is imperceptible or nearly imperceptible to the user, yet may be detected through an automated detection process. Watermarking is the art of imperceptibly embedding a message into a work. More than 700 years ago in Fabriano (Italy), paper watermarks appeared in handmade paper, in order to identify its provenance, format, and quality. In this context, the watermark is a kind of invisible signature that allows identifying the creator or the owner of a document, and to detect possible copyright violations, and especially non-authorized copying [1]. More recently, different watermarking techniques and strategies have been proposed in order to solve a number of problems, ranging from the detection of content manipulations, to information hiding (steganography), to document usage tracing. In particular, the insertion of multiple watermarks to trace a document during its lifecycle is a very interesting and challenging application [1]. The main property of the proposed method is that it allows the insertion of multiple watermarks by different users, who sequentially come into play one after the other and do not need any extra information besides the public keys. This characteristic makes the present approach more attractive than previously available solutions.

Keywords: VSPM, QIM, ACE, CLS, DFD, UML, HTML etc.

I. INTRODUCTION OF WATERMARKING

One of the biggest technological events of the last two decades was the invasion of digital media in an entire range of everyday life aspects. Digital data can be stored efficiently and with a very high quality, and it can be manipulated very easily using computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality. Digital media offer several distinct advantages over analog media. The quality of digital audio, images and video signals are better than that of their analog counterparts. Editing is easy because one can access the exact discrete locations that need to be changed. Copying is simple with no loss of fidelity and a copy of a digital media is identical to the original. With digital multimedia distribution over World Wide Web, Intellectual Property Right (IPR) are more threatened than ever due to the possibility of unlimited copying [11].

A Watermarking is adding “ownership” information in multimedia contents to prove the authenticity. This technology embeds a data, an unperceivable digital code, namely the watermark, carrying information about the copyright status of the work to be protected [3]. Continuous efforts are being made to device an efficient watermarking schema but techniques proposed so far do not seem to be robust to all possible attacks and multimedia data processing operations.

Generally, the watermarking of still image, video, and audio demonstrate certain common fundamental concepts. Numerous watermarking applications reported in the literature depend on the services we wish to support. Thus watermarking techniques may be relevant in various application areas including Copyright protection, Copy protection, Temper detection, Fingerprinting, etc.

A. Existing System
The existing method only did single water marking. That will not give that much security to image. The general problem of multiple digital watermarking has been the object of several investigations since the pioneering contribution. It is suggested that the insertion of multiple watermarks can be exploited to convey multiple sets of information. More recently, a multiple watermark-embedding procedure was proposed, which allows simultaneous insertions without requiring the key sets to be orthogonal to each other.

B. Proposed System
In this paper, we introduce a new approach that allows the tracing and property sharing of image documents thanks to the possibility of sequentially embedding multiple watermarks into the data [1]. It is intended for the detection and insertion of watermarks into digital image [2]. The main property of the proposed method is that it allows the insertion of multiple watermarks by different users, who sequentially come into play one after the other and do not need any extra information besides the public keys. This characteristic makes the present approach more attractive than previously available solutions.

Thus I had implemented here a watermarking scheme, which allows inserting and reliably detecting multiple watermarks sequentially embedded into a digital image, as it is a challenging task in Digital Image Processing.

II. BASIC CONCEPT
Based on their embedding domain, watermarking schemes can be classified either as Spatial Domain (The watermarking system directly alters the main data elements, like pixels in an image, to hide the watermark data) or Transformed Domain (the watermarking system alters the frequency transforms of data elements to hide the watermark data) [3]. To transfer an image to its frequency representation, one can use several reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT). Each of these transforms has its own characteristics.
and represents the image in different ways. Watermarks can be embedded within images by modifying these values, i.e. the transform domain coefficients. In case of spatial domain, simple watermarks could be embedded in the images by modifying the pixel values or the least significant bit (LSB) values.

A. Implementation

Digital watermarking systems typically have two primary components: an encoder that embeds the watermark in a host media signal, and a decoder that detects and reads the embedded watermark from a signal suspected of containing a watermark (a suspect signal). The encoder embeds a watermark by altering the host media signal. The reading component analyzes a suspect signal to detect whether a watermark is present. In applications where the watermark encodes information, the reader extracts this information from the detected watermark.

One particular problem in digital watermarking applications is synchronizing a detector to deal with geometric warping distortion of a watermarked image. A number of techniques have been developed for dealing with geometric distortion in watermarked images. One technique is to make the watermark more robust to geometric distortion by embedding it in attributes of the image that are relatively invariant to geometric distortion. While this improves detection in some cases, it typically does not address all forms of geometric distortion and more complex, non-linear geometric distortion.

B. Image Watermarking Algorithm

1. Start
2. Read original image
3. Read sample image to add as watermark.
4. X, Y Positions of Watermark sample image into original image.
5. Draw Sample image onto original as watermark.
7. Stop

C. Testing Results

<table>
<thead>
<tr>
<th>Test Case #</th>
<th>Test Case Description</th>
<th>Expected Results</th>
<th>Pass/Fail</th>
<th>Actual Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Click on change open in file menu.</td>
<td>It should open the open dialog box</td>
<td>Pass</td>
<td>It has opened the open dialog box.</td>
</tr>
<tr>
<td>02</td>
<td>Click on open button without selecting an image.</td>
<td>It should ask for select an image.</td>
<td>Pass</td>
<td>It has showing error message for “you should select an image”</td>
</tr>
<tr>
<td>03</td>
<td>Select an image from the open dialog box.</td>
<td>It should be redirect to other form.</td>
<td>Pass</td>
<td>It should be redirect to other form.</td>
</tr>
</tbody>
</table>

Table 1: Image Selection Form

D. TESTING TYPES

1) Specification Testing
This is done to check if the program does what it should do and how it should behave under various conditions or combination and submitted for processing in the system and it is checked if any overlaps occur during the processing.

2) Performance Time Testing
This is done to determine how long it takes to accept and respond i.e., the total time for processing when it has to handle quite a large number of records. It is essential to check the exception speed of the system, which runs well with only a handful of test transactions. Such systems might be slow when fully loaded. So testing is done by providing large number of data for processing. A system testing is designed to uncover weaknesses that were not detected in the earlier tests.

III. CONCLUSION

Having described and illustrated the principles of the technology with reference to specific implementations, it will be recognized that the technology can be implemented in many other, different, forms. The methods, processes, and systems described above may be implemented in hardware, software or a combination of hardware and software. The particular combinations of elements and features in the above detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this and the incorporated by reference patents/applications are also contemplated.

ACKNOWLEDGEMENT

The success of this research depends largely on the encouragement and guidelines of many others. We take this opportunity to express my gratitude to the people who have been instrumental in the successful completion of this research. We would like to show my greatest appreciation to Assistant Prof Priyanka Trikha. Without her encouragement and guidance this work would not have materialized. The guidance and support received from all of my friends and all our faculty members who give their valuable suggestions to me for this research. I am grateful for their constant support and help.
REFERENCES

[1] Giulia Boato, Member, IEEE, Francesco G. B. De Natale, Senior Member, IEEE, and Claudio Fontanari

[2] Oktay Altun, Gaurav Sharma and Mark Bocko ECE Department, University Of Rochester, Rochester, NY, 14627


