LSB Based Image Watermarking with Hybrid Compression-Encryption Technique

Shaista Qureshi\textsuperscript{a*}, Sreeja Nair (Guide) \textsuperscript{b}

\textsuperscript{a, b} Department of Computer Science and Engineering, Oriental Institute of Science and Technology, Bhopal-24, India

Abstract

Security plays an important role during the transmission of message or multimedia data from sender to receiver. Although there are various techniques implemented for the security of these data i.e. through authentication or cryptography. But watermarking is one of the possible way of securely transmitted the data to the receiver by hiding information behind the image. Here in this paper we implement a combinatorial method of compression, encryption and watermarking of image. The concept of encryption in watermarking provides more security to the watermarked image where the detection of information is difficult while compression is used to save the bandwidth of the data during transmission.

Keywords: Compressed and Encrypted Domain Watermarking, JPEG2000Watermarking, Robust.

1. Introduction

The digital revolution and the explosion of communication networks, and the increasingly mounting passion of the general public for new information technologies lead to exponential growth of multimedia document traffic (image, text, audio, video, etc.). This occurrence is now so important that insuring protection and control of the exchanged data has become a foremost issue. Definitely, from their digital scenery, multimedia documents can be easily duplicated, modified, altered, and diffused very simply. In this context, it is important to extend systems for copyright defence, protection against repetition. Multimedia data security and authentication can be achieved by compression and encryption whereas watermarking is also an alternative solution for reinforcing the security of multimedia documents.

1.1 Basic Watermarking Principles

It would be then achievable to recover the embedded message at any time, even if the document was misrepresented by one or more non-destructive attacks, that can be either malicious or not. Until now, the preponderance of publications in the field of watermarking primarily addresses the copyright of still images. Supplementary security services, such as image based authentication, are still insignificant and many essential questions remain open. It may wonder, for example, whether it is preferable to use a fragile watermark, a robust watermark, or still use a completely diverse technique. Furthermore, an authentication service moderately calls into question the settings commonly established in watermarking copyright protection, predominantly in terms of the quantity and nature of hidden information (for copyright, the mark or blot is independent of the image and is typically a 64-bit identifier), as well as in terms of robustness [2].

1.2 Watermarking verification and Detection Method

Non-blind

In non-blind watermarking technique original image is required during the watermarking of the image.

Semi-blind

In this watermarking technique the watermarking requires some of the data information and the original image.

\textsuperscript{*} Corresponding Author Email: shaista.qureshi17@gmail.com
Blind

In this technique during the watermarking of the image it neither requires original data nor some of the data information.

1.3 Generic Watermarking System

Digital watermarking algorithms contain three parts, watermark embedding algorithm, watermark extraction algorithm and watermark detection algorithm [12]. A general watermark system phases is shown in Figure 2.

The watermark lifecycle phases consist of attack function which may be applied for the embedding and detection of watermark in images. The Attack function used here may be made secure so that the chances of attack in the image to read the information hiding are accessible.

Watermark attacks can be classified as:

Simple Attacks: In this type of attack the attacker may try to damage the watermark embedded in the image by adding some noise or by making the image corrupted.

Detection-disabling Attack: Although there are many techniques used for the detection of watermarking in images, in this type of attack the attacker may try to change the geometry of the image by scaling or permutation.

Ambiguity Attack: In this attack the attacker embeds some fake watermark which creates ambiguity between the real watermarked signal and the fake watermark signals.

Removal Attack: Here in this attack the attacker can detect the watermark embedded in image and discard the embedded signal by applying some collusion attack or some conceptual cryptographic weakness.

1.4 Philosophy of Integrity

In the security society, an integrity service is explicitly defined as one, which insures that the transmitted and received data are identical. This binary definition can also be appropriate to images; however it is too strict and not well tailored to this type of digital document. Certainly, in real life situations, images will be malformed. Their pixel values will therefore be tailored but not the actual semantic meaning of the image. In other words, the difficulty of image based authentication concerns the image content, such as, when modifications of the document may change its sense or visually degrade it. Hence to provide an efficient authentication of the contents of image the watermarking techniques applied should be made secure enough to secure the embedded text in the image so that the technique is efficient.

1.5 LSB Encoding

The best known Watermarking method that works in the Spatial Domain is the Least Significant Bit (LSB), which replaces the least significant bits of pixels selected to hide the information. Least significant bit watermarking method has several implementation versions that improve the algorithm in certain aspects.

It consists of four phases:

a. Generation
b. Embedding
c. Distribution and attacks.
d. Detection and recovery.

In Generation stage watermark is created and its contents should be unique and complex such that it is difficult to extract or damaged from possible attacks. In Embedding stage watermark is embedded in cover image. Embedding is directly related to extraction algorithm. Therefore Embedding algorithm is combination of watermark with chosen media, so the result is equivalently:

\[ WM = E (CI, WI) \]

Where; CI is original image, WI is watermark, E is embedding function and WM is the watermarked media. The Distribution process can be seen as transmission of signal through watermark channel. Possible attacks in broadcast channel may be intentional or accidental. Detection process allows owner to be identified and provides information to the intended recipients. There are two kinds of detection: Informed detection and Blind detection. To insert a watermark we can use spatial domain and transform domain.

2. Related Work

A.V. Subramanyam, Sabu Emmanuel [3] proposed a robust watermarking technique for jpeg2000 image. The technique uses the concept of first encrypted the image using RC4 encryption technique and then applying jpeg200 compression for the image compression and hence applying watermarking embedding in the compressed image. Here in this paper three watermark techniques are given based on Spread Spectrum (SS), Scalar Costa Scheme Quantization Index Modulation (SCS-QIM), and Rational Dither Modulation (RDM).

In paper titled “compressed-encrypted domain jpeg2000 image watermarking” by A. V. Subramanyam, Sabu Emmanuel, Mohan S. Kankanhalli [4] suggested an efficient way of embedding the watermarking either by first applying the compression or encryption and is performed on jpeg2000 image. The techniques provide detection of
the watermarking at the time of the compression or encryption of the image. The technique is simple to implement and is efficient as per security is concerned. The technique uses jpeg2000 compression algorithm for the compression of image and stream cipher using RC4 is used for the encryption of the image and the watermark signal generation and detection is done by using spread spectrum technique.

Anamitra Makur, Nikhil Narayan S. [5] presented a watermarking technique including DCT based compression as an application for the image tempering. The technique uses spread spectrum based watermarking technique which is a fragile watermarking technique. The idea is to detect tamper and provides recovery of images where we do not require authentication bits.

In the paper “Feature-based Watermarking using Discrete Orthogonal Hahn Moment Invariants” Shiraz Ahmad [6] purport a new robust technique for the watermark images that may be attacked using some geometric transformation of image such as scaling or rotation. The watermarked embedding can be easily detection by transformation of image. Hence proposes a technique to prevent from such attacks by using scale invariant feature transform based bounding boxes and moment-invariant for the watermark embedding which can prevent from geometric attacks.

A watermark technique is proposed which is used for the recovery of tampered documents [7]. The technique is used for the recovery of the documents using pixel flipping and then self-embedding so that the authentication is achieved. This technique recovers against all types of attacks possible in tampered document such as insertion or substitution or deletion.

Soumya Mukherjee, Arup Kumar Pal proposed a new technique of water marking using the combinatorial method of discrete wavelet transform and singular value decomposition on gray scale images. The technique implemented here for watermarking is suitable to prevent the gray images from various attacks such as nosing, cropping or image enhancement.

Digital video watermarking is proposed by Ujan Mukhopadhyay, Souptik Sinha, Poulomi Ghosh, Rilok Ghosh, Dipak kr. Kole and Aruna Chakroborty [9] Although there many watermarking techniques implemented for the video, here a new technique has been implemented where the video is first divide into a number of frames and a key is used which is applied on each frame for the encryption of the frames and the same key is then applied for the decryption of video frames and the frames are then arranged to get the original video in a secure way.

A digital image watermarking technique has been implemented [10] in which one quad tree based approach is used to select the region of interest (ROI) and then to utilize the properties of the singular value decomposition (SVD) transform to hide the watermark is being proposed here.

A blind watermarking technique has been proposed using the concept of DCT [11]. Here the watermarking using DCT can be given by calculating correlation coefficient between the extracted coefficients of the watermarked image and then the partial watermark values that are known are calculated.

3. Proposed Methodology

Load an image as an input. Filter the image using Gaussian filter and find the histogram of the image. The reason behind using JPEG-LS compression technique is that at the decompression side the image obtained will be identical to original image, i.e. no data will be lost. JPEG-LS achieve significantly better compression results than those obtained with other (nonstandard) algorithms previously investigated for the compression of elevation data. Further encrypt the image using AES algorithm. The Advanced Encryption Standard (AES) is a symmetric-key block cipher encryption technique which works on block of data not on individual bite or bytes. AES has a block size of 128 bits. AES has defined three versions, with 10, 12, and 14 rounds. Each version uses a different cipher key size (128, 192, or 256), but the round keys are always 128 bits.

![AES encryption design](image)

Each round has 4 steps: (a) Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table. (b) Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps. (c) Mix Columns—a mixing operation which operates on the columns of the state, by combining the four bytes in each column. (d) Add Round Key - round key is always of 128 bits. And Final Round (no Mix Columns) has only 3 steps: Sub Bytes Shift Rows and Add Round Key. Now Embed watermarking technique on the compressed encrypted. We will perform LSB (least significant bit) watermarking on the image. Previously the watermarking was used to done at the frequency or at intensity domain. We here perform image watermarking using LSB of image. The idea behind this watermarking technique is that if we see our image as a
matrix \( N \times M \) (where \( N \) and \( M \) are the dimension of the image) we can represent the value of the pixel as a binary number, so that you will have a most significant bit (the one that contains quite a lot of information, and least significant bit that contains few information). Now authenticate the user using the watermarking embedded in the image. The authentication is done by using the secret key generated at the encryption stage. So that we can come to know that the decrypting party is authenticate user and not an unauthenticated one. The watermark detection can be done either in encrypted domain or in decrypted domain. Decrypt the image and then apply decompression to get the original image. The decompression process will be the reverse of compression process. Find the histogram of the image and compare it with the original image.

4. Result Analysis

This section will discuss about the result generated by processing images. Given tables and figures shows the result setup for the comparison between base and existing work. Table 1 fshow the base work with 2 different images i.e. woman and lena having .jpg or .jpeg extention. The result analysis is given below by using 4 parameters, numbers of colors, mean square error, NCC, NAE. The unit of error is dB decible. MSE is the error metrics used to compare image compression quality. Table 2 Here in table 5.2 we are demonstrating the comparison between the base work and propose work considering three parameters CPU time, PSNR, Payload Capacity.

CPU time is the time taken by the CPU to perform the whole task from initialization upto termination. Its unit is second (sec). Payload bit or capacity is the the ratio of the average embedded number of bits to the average compressed stream size (in bytes), where average is computed as a simple mean. Db is decibel, the unit of noise signal.

<table>
<thead>
<tr>
<th>Image</th>
<th>No. of Colors</th>
<th>Mean square Error</th>
<th>NCC</th>
<th>NAE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Woman</td>
<td>254</td>
<td>1.6640e+004</td>
<td>4.3038e-004</td>
<td>1.0005</td>
</tr>
<tr>
<td>Lena</td>
<td>239</td>
<td>1.5703e+004</td>
<td>7.2774e-004</td>
<td>1.0004</td>
</tr>
<tr>
<td>Satellite</td>
<td>256</td>
<td>9.6003e+003</td>
<td>-0.0016</td>
<td>1.0042</td>
</tr>
</tbody>
</table>

![Figure 3 (a) Watermark embedding (b) watermark detection](image)

**3.1. LSB algorithm**

The least significant bit (LSB) technique is used to embed information in a cover image. The LSB technique is that inside of a cover image, pixels are changed by bits of the secret message. These changes cannot be perceived by the human visibility system. However a passive attacker can easily extract the changed bits, since it has performed very simple operation.

After the secret data gets embedded or hidden in the cover image, the original cover image will get modified to some extent with respect to the length of the secret data. At the receiving end we are not able to get back the original cover image since our traditional LSB is not providing reversibility. Reversible feature is a process of getting back the cover image from the watermarked or embedded image at the extraction phase. After getting the watermarked image, we need to create a matrix initialized with zeros, whose dimension is equal to the watermarked image. By XORing each and every pixel of both the original and watermarked image, the result will be stored in the corresponding positions in the newly created matrix. This matrix will also be sent to the extraction phase along with the watermarked image. During extraction the value of the newly created matrix will be checked. If it is 1, then watermarked image’s s LSB of each pixel must be changed, else vice versa. Finally we could get back to the original cover image.
which allows us to detect the watermark after decryption and control the image quality as well.

References