Secure Digital Image Watermarking using DWT, SVD and Chaotic Encryption with Genetic Algorithm

Roshan Jahan\(^1\), Preetam Suman\(^2\)
roshan@iul.ac.in, preetam.suman@ieee.org

Abstract

Watermarking is very useful to secure multimedia and personal data. The protection of watermark image is an issue these days. There are various threats occurs which can change watermark image. This paper is proposing a security mechanism for watermark image using DWT-SVD and optimized chaotic based image encryption through genetic algorithm with high level of robustness and security. The proposed mechanism is implemented on MATLAB, and tested in presence of various attacks. The algorithm is very efficient with respect to other security mechanism. The results are discussed in the paper.

Keywords: Watermarking, Gaussian noise, salt and pepper noise, DWT.

Introduction

Digital multimedia data are not safer these days because possibility of duplication or manipulation of the data [1]. Reliable transmission of digital data needs a technique to preserve and secure the data. [2].

There are few approaches designed for protecting data and securing systems. One of them is data encryption (cryptography) [3]. The key distribution is one of the approaches. Encrypted data can be decrypt only using the key. But distribution of key is not secure [4]. The other technique is steganography. It was derived from Greek, literally means “covered writing” is the art of hiding information inside other data in ways that prevent the detection of hidden message. Watermarking is other reliable technique for security of digital data [5, 6]. It is a hidden method to protect digital data. There are various applications of watermarking like copyright protection, fingerprinting, copy protection, broadcast monitoring, data authentication, indexing, medical safety, and data hiding.

\(^1\), \(^2\) Assistant Professor, CSE Department, Integral University, Kursi Road, Lucknow, UP, India
There are various literatures available on security of watermark images. It provides right direction to perform research on various techniques.

Qing Liu et al. [7] proposed a method to reduce effect of attack on watermark image. This method was based on superimposing digital watermarking principle and wavelet multi-resolution analysis, adaptive blind grayscale image watermarking algorithm. Author has implemented the method and tested it. The result shows that the proposed algorithm is able to defend the attacks on watermark images.

Chaofan Peng et al. [8] described the preliminary study and exploration of dynamic watermarking scheme on the basis of software watermarking technology and analysis the process of dynamic graph watermarking. Author also proposed the IPPCT dynamic watermarking scheme based on Chinese remainder theorem. In the research paper author has described the stages of watermarking embedding, decomposition, encryption and identification. The experimental results show that the new scheme was efficient in protection of watermark image.

Moniruzzaman et al. [9] proposed a technique to protect patient information in medical images. The technique was based on discrete wavelet transform (DWT) domain and chaotic system based medical image watermarking scheme. Author has also compared experimental results of the proposed method with existing algorithms. The proposed method was better than existing algorithms.

Umaa maheshvari et. al. [10] proposed a mechanism to improve the embedding phase based on convolution code to improve the robustness of the embedded watermark. The proposed watermarking technique is preferred in low frequency band of the Discrete Wavelet Transform (DWT) and as a result it can refuse to accept the destruction of image processing. The parameters for evaluation of proposed algorithm were PSNR, MSE, SSIM, Correlation, and Entropy. Experimental results show that this proposed watermarking technique is more robust than the existing method.

Dhole et. al. [11] introduced a modified fragile watermarking technique for image recovery to detect and recover the tampered image with its tampered region. The author has focused on provide resistance on various attacks like birthday attack, college attack and quantization attacks. In this modified technique author put a watermark information and information of recovery of image block into the image block. These blocks are linked with next randomly generated block of image. The results show that, the proposed technique can be used as an alternative approach to image recovery.

Moniruzzaman et al. [12] has proposed a scheme based on fragile watermarking scheme based on chaotic system. Two dimensional Arnold's cat map has been used to improve the security of the proposed watermarking scheme. Arnold's cat map is used to obtain the scrambled image by shuffling the pixel positions of the image. From the experimental results it can be observed that the proposed watermarking scheme gives better results than other chaos based watermarking schemes.

Organization of paper: section II describes attacks on images, proposed methodology is described in section III, section IV presents results and then conclusion is discussed in section V.
Attacks on Images

There are various types of attacks performed by attackers [13, 14]. Few of them are following:
1) Active attacks: In this attack intruder remove all security watermarks or change it according to him.
2) Passive attacks: In this attack attacker is not trying to remove the watermark but simply attempting to determine if a given mark is present or not.
3) Collusion attacks: In this type of attacks, the goal of the hacker is to remove the watermark, using several copies of the same data, containing each different watermark, each signed with a key, to construct a new copy without any watermark.
4) Forgery attacks: In this attack the hacker tries to embed a new, valid watermark rather than removing it.
5) Ambiguity attacks: These are attacks that attempt to embed one or several additional watermarks such that it is unclear which the first authoritative watermark was.
6) Protocol attacks: Protocol attacks aim at attacking the entire concept of the watermarking application.
7) Gaussian Noise Attack: In this attack original image becomes blur image.
8) Salt and pepper attack: An image containing salt-and-pepper noise will have dark pixels in bright regions and bright pixels in dark regions.
9) Multiplicative Noise: Multiplicative noise refers to an unwanted random signal that gets multiplied into some relevant signal during capture, transmission, or other processing.

Methodology

Discrete Wavelet Transform (DWT) is a multiresolution analytical approach of time-frequency and can describe partial characteristics of time and frequency domains. The basic thought is to decompose the image to sub images with different space and frequency, then the coefficient is processed.

The DWT can be implemented as a multistage transformation. An image is decomposed into four sub-bands denoted as LL, LH, HL, and HH in DWT domain, where LH, HL, and HH represent the finest scale wavelet coefficients and LL stands for the coarse-level coefficients.
Proposed model for watermark embedding:

![Block diagram of proposed model for watermark embedding](image)

**Step 1:** The first step of the model is to perform one-level Haar Discrete Wavelet Transform which is used to divide the cover image into four non-overlapping multi-resolution sub-bands (i.e., LL, LH, HL, and HH).

![Input image and one level Haar DWT](image)

![Result of step 2](image)

**Step 2:** Now perform Singular Value Decomposition to LH and HL subbands, i.e.,

$$\mathbf{I}_n = \mathbf{U}_n \mathbf{S}_n \mathbf{V}_n^T, n = 1, 2$$  \hfill (1)

Where, n represents sub-bands.

**Step 3:** Decompose the watermark image into two parts: $W = W_1 + W_2$.

Where, $W_n$ denotes half of the watermark.
Step 4: Modify the singular values in HL and LH subbands with half of the watermark image and then apply SVD to them, respectively, i.e.,

$$S_n + \alpha^*W_n = U_{nw}S_{nw}V_{nw}^T$$ (2)

Where, $\alpha$ denotes the scale factor. The scale factor is used to control the strength of the watermark to be inserted.

Step 5: Apply the given method to obtain the two sets of modified DWT coefficients, i.e.,

$$I_n^* = U_nS_nV_n^T, \ n= 1, 2$$ (3)

Step 6: Now by performing the inverse DWT, obtain the watermarked image $IW$ using two sets of modified DWT (i.e LH & HL) coefficients and two sets of unmodified DWT (LL & HH) coefficients.
Proposed Model for Watermark Extraction:

![Block diagram of proposed model for watermark extraction](image)

Step 1: Perform one-level Haar DWT to divide the watermarked (possibly distorted) image $I^W$ into four sub bands (i.e. LL, LH, HL, and HH.)

![One level Haar output of image](image)

![Singular Value Decomposition to LH and HL sub bands](image)

Step 2: Perform Singular Value Decomposition to LH and HL sub bands, i.e.,

$$I^W_n = U^W_n S^W_n V^W_n T, \quad n = 1, 2 \ (4)$$

Where, $n$ represents one of two sub-bands.

Step 3: Compute $E^W_n = U^W_n S^W_n V^W_n T$, $n = 1, 2$
Roshan Jahan, Preetam Suman

Secure digital image watermarking using DWT, SVD and chaotic encryption with Genetic Algorithm

Step 4: Now Extract half of the watermark image from each sub-band, i.e.,

\[ W^n = \frac{E^n - S_n}{\alpha}, \quad n = 1, 2 \]  

(5)

Step 5: Combine the results of Step 4 to obtain the embedded watermark:

\[ W = W^1 + W^2 \]

Proposed model for secure watermark: The proposed model for secured watermark is the combined approach of image watermarking which have been used that satisfies two requirements i.e. imperceptibility and robustness.

The watermarking method consists of combination of discrete wavelet transform (DWT) and singular value decomposition.
The encryption method used for the watermark image is combination of a genetic algorithm and chaotic function. Every time an encrypted image with the highest entropy and the lowest correlation coefficient among adjacent pixels is produced.

Results

Algorithm has been tested on standard image of Leena and Cameraman. In this paper image of ‘Lena’ was used as cover image and image of ‘cameraman’ was used as watermark image.

The following parameters were used for evaluation.

- Peak signal-to noise ratio (PSNR)
- Normalized Cross-Correlation (NC)
- Correlation coefficient (CC) and
- Histogram Deviation (HD)

The algorithm has been evaluated in presence of following attacks:

- Gaussian noise (GN)
- Salt & Pepper (SP)
- Multiplicative Noise(MN)

Figure 15 is showing images and effect of watermarking on original image.
Figure 15: (a) Leena image (b) Photographer image as watermark, (c) Encrypted watermark image, (d) Watermarked image and (e) extracted and decrypted watermark image.

Results in absence of Attacks:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Psnr</td>
<td>39.3673</td>
</tr>
<tr>
<td>Psnr1</td>
<td>58.7429</td>
</tr>
<tr>
<td>NC</td>
<td>1</td>
</tr>
<tr>
<td>CRbest</td>
<td>-0.0741</td>
</tr>
<tr>
<td>HD</td>
<td>2.9999</td>
</tr>
</tbody>
</table>

Table 1: Results in absence of Attacks on Image
Results in presence of Attacks on Image

<table>
<thead>
<tr>
<th></th>
<th>Gaussian Noise Attack</th>
<th>Salt and pepper attack</th>
<th>Multiplicative Noise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Psnr</strong></td>
<td>G=0.001</td>
<td>G=0.01</td>
<td>G=0.1</td>
</tr>
<tr>
<td></td>
<td>30.7182</td>
<td>30.6911</td>
<td>33.2083</td>
</tr>
<tr>
<td><strong>Psnr1</strong></td>
<td>S=0.005</td>
<td>S=0.05</td>
<td>S=0.1</td>
</tr>
<tr>
<td></td>
<td>50.0706</td>
<td>40.5358</td>
<td>32.6545</td>
</tr>
<tr>
<td></td>
<td>Mn=0.004</td>
<td>Mn=0.04</td>
<td>Mn=0.1</td>
</tr>
<tr>
<td></td>
<td>30.6702</td>
<td>29.4167</td>
<td>27.7171</td>
</tr>
<tr>
<td><strong>NC</strong></td>
<td>0.8974</td>
<td>0.8140</td>
<td>0.7928</td>
</tr>
<tr>
<td></td>
<td>0.9982</td>
<td>0.8110</td>
<td>0.8788</td>
</tr>
<tr>
<td></td>
<td>0.8147</td>
<td>0.8118</td>
<td>0.6159</td>
</tr>
<tr>
<td><strong>Crbest</strong></td>
<td>0.0682</td>
<td>0.0571</td>
<td>0.0566</td>
</tr>
<tr>
<td></td>
<td>0.0638</td>
<td>-0.0554</td>
<td>-0.0736</td>
</tr>
<tr>
<td></td>
<td>-0.0553</td>
<td>-0.0601</td>
<td>-0.0581</td>
</tr>
</tbody>
</table>

Table 2: Result of proposed mechanism in presence of noise

Conclusion

Security of multimedia data is very important. Watermarking is the one of the best method to provide security on images. A security mechanism for watermark image is discussed in this paper using DWT-SVD and optimized chaotic based image encryption through genetic algorithm with high level of robustness and security. The proposed mechanism was implemented on MATLAB, and tested in presence of various attacks. The mechanism is able to reduce effects of Gaussian noise (GN), Salt & Pepper (SP), and Multiplicative Noise (MN).

References:


This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0/).

© 2015 by the Authors. Licensed by HCTL Open, India.