Data Hiding in Watermarking Technique with Effective Key Length Using Spread Spectrum Technique

S. Poongodi and Dr. B. Kalaavathi

1Assistant Professor, Department of ECE, K.S.R. College of Engineering, Anna University, Chennai, Tamilnadu, India
2Prof & Head, Department of CSE, K.S.R Institute for Engineering and Technology, Anna University, Chennai, Tamilnadu, India

ARTICLE INFO

Article history:
Received 25 June 2014
Received in revised form 8 July 2014
Accepted 25 August July 2014
Available online 29 September 2014

Keywords:
Spread Spectrum (SS), Effective Key Length, Peak to Signal Noise Ratio (PSNR), Mean Square Error (MSE)

ABSTRACT

The principle of watermarking is to transmit the data in a protected manner over the text, audio and video processing. The embedding and extraction of the hidden data is taken using the secret key from an object. A new measure of Effective key length is used to transmit the data in an efficient manner. Effective key length is processing of inserting the secret key randomly through the any of the pixels in an image and then the watermarked is to be transmitted. This methodology is applied here with Additive Spread Spectrum (SS) scheme which the effective key length is proposed. The data is inserted into an image using the secret key and then this watermarked image is embedded into the original image using the DWT process. Some of the parameters like Peak to Signal Noise Ratio (PSNR), Mean Square Error (MSE) and Time taken for the embedding and extraction of watermarking process is to be measured.

INTRODUCTION

Digital watermarking is that technology that provides and ensures security, data authentication and copyright protection to the digital media. Watermarking techniques is achieved through the Spread Spectrum (SS). In most watermarking schemes spread spectrum (SS) is the modulation technique used to embed the watermark. In this case the signal to be marked (the carrier signal) acts as a source of interference. Because the carrier signal itself is generally much stronger than other interference, its interference dominates the performance of watermark detection. A new methodology to estimate the security levels of watermarking schemes based on the definition of equivalent keys, the probability of finding such an equivalent key, and its translation in bits. There are the keys allowing a reliable decoding of content watermarked with the secret key. The security is in direct relationship with the length of the secret key, which is a binary word of L bits. The length of the keys L is the entropy in bits if the keys are uniformly distributed but it is also the maximum number of tests in logarithmic scale of the brute force attack which finds the key by scanning the K potential keys.

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL). The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution.

MATERIALS AND METHODS

A. Digital Image Watermarking:

Digital watermarking is that technology that provides and ensures security, data authentication and copyright protection to the digital media. Digital watermarking is the embedding of signal, secret information
Digital watermarking hides the copyright information into the digital data through certain algorithm. The secret information to be embedded can be some text, author’s serial number, company logo, images with some special importance. The watermark can be hidden in the digital data either visibly or invisibly. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain. Both the domains are different and have their own pros and cons and are used in different scenario.

B. Frequency Domain Watermarking:

Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients. Some of its main algorithms are discussed below:

C. Discrete Wavelet Transformation (DWT):

The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well. The 2-D discrete wavelet transforms (DWT) decomposes the image into sub-images, 3 details and 1 approximation. The approximation looks just like the original; only on 1/4 the scale. The 2-D DWT is an application of the 1-D DWT in both the horizontal and the vertical directions. The DWT separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components.

In watermarking security the DWT process places an important role in hiding the data into the image for transmission and then process of adding the data into the image through the pixels. This property allows the exploitation of the masking effect of the human visual system such that if a DWT co-efficient is modified, it modifies only the region corresponding to that coefficient. The embedding watermark in the lower frequency sub-bands may degrade the image as generally most of the Image energy is stored in these sub-bands. However it is more robust. The high frequency part contains information about the edge of the image so this frequency sub-bands are usually used for watermarking since the human eye is less sensitive to changes in edges so this frequency sub-bands.

![Host Image](image)

**Fig 1:** Shows 2 level of decomposition.

C. Spread Spectrum Watermarking:

In most watermarking schemes, spread spectrum (SS) is the modulation technique used to embed the watermark. In this case, the signal to be marked (the carrier signal) acts as a source of interference. Because the carrier signal itself is generally much stronger than other interferences, its interference dominates the performance of watermark detection. Practically any watermarking system currently using SS would immediately profit from using the proposed scheme. Gains will vary according to signal-to-noise ratio (SNR) and current error probability, but improvements of 20 dB in noise immunity or reduction in error probabilities of 20 orders of magnitude can be achieved.
**Security Is Measured By the Effective Key Length:**

In symmetric cryptography, the security is in direct relationship with the length of the secret key, which is a binary word of \( L \) bits. The length of the keys \( L \) is the entropy in bits if the keys are uniformly distributed but it is also the maximum number of tests in logarithmic scale of the brute force attack which finds the key by scanning the \([K]\) potential keys. If the adversary draws a key uniformly, the probability to pick the secret key is \( P = 2^{-L} \) or in logarithmic scale, \( L = -\log_2(P) \). A good cryptosystem has a security close to the length of the key \( L \). For instance, the best attack so far on one version of the Advanced Encryption Standard using 128 bits secret key offers a computational complexity of \( 2^{126.4} \).

The notion of key length to watermarking thanks to the brute force attack scenario. A naive strategy is to take the size of the seed of the pseudo-random generator as it is the maximum number of tests of a brute force attack scanning all the seeds. Yet, it doesn’t take into account how the secret key is derived from the seed, and especially whether two seeds leads to very similar secret keys.

In a first step, the adversary, modeled by a probabilistic polynomial-time Turing machine, observes contents watermarked with the secret key \( k_1 \) or \( k_2 \). Then, the designer produces a new piece of content \( y \) and challenges the adversary whether \( y \) has been watermarked with key \( k_1 \) or \( k_2 \). The advantage is defined as the probability of a right guess minus \( 1/2 \). One clearly sees that a strictly positive advantage implies that the adversary has been able to infer some information about the secret key during the first step.

**Mathematical Analysis of The Effective Key Length For SS And ISS:**

The mathematical expression which analyze the tradeoff between the robustness vs. security and then the new approach applied to one of the most popular class of watermarking schemes: Spread Spectrum(SS) and Improved Spread Spectrum(ISS).

The embedding is parameterized by \((\beta,\gamma)\),

\[
y = e(x,y,z) = x + ((-1)^\beta - \gamma (x^T k))K
\]

The decoding is given by the sign of the correlation \( d_e = K^T y \). To evaluate the robustness, we addition of an independent white Gaussian noise \( n \sim N(0,\sigma_n^2) \). Thanks to a symmetry argument, we only need to consider one message, say \( m = 0 \). There is a decoding error if \( d_e = K^T n + (1 - \gamma) K^T x + B \) is negative. Signals \( n \) and \( x \) being independent, we obtain:

\[
\eta(\sigma_n) = \phi \sqrt{\frac{D y^2 \sigma_x^2}{(1-\gamma)^2 \sigma_x^2 + \sigma_n^2}}
\]

\( \phi(\cdot) \) being the cumulative distribution function of the Gaussian random variable, the function \( \phi = -\sqrt{\cdot} \) is a decreasing function.

**RESULTS AND DISCUSSION**

The input image is taken as the lena image and cameraman image in which the data or an kind of hidden part is taken as the input data to be hidden. The image and data are combined through the process of DWT. Effective key length is process of creating the secret key \( K \) for hiding of an image and then the probability of finding the equivalent key of an image. Then the watermark image is inserted into the other image for transmission. Then at the reception side the watermarked image recovered from the transmitted image and then secret key is given to extract the watermark image which contains image and data. The following process discusses about the embedding and extraction of watermarking technique and results are shown below.

The process of embedding the data and the image is carried out through the following steps,

- **Step 1:** The host image is taken as the input image for inserting the data.
- **Step 2:** The data is added into the image using the DWT process of separation pixels and then the data is added through binary values.
- **Step 3:** Image that contained hidden data is referred to as watermark image.
- **Step 4:** Secret key is given to the watermark image for make the image to be secured using DWT process is referred to as watermarked image.
- **Step 5:** The watermarked image is again inserted into the image for transmission of image over an media.
Fig 2: Lena input image and watermarked image with embedded data.

Fig 3: secret key is given to that image and image after retrieval of data when secret key is given

Fig 4: Watermarked cameraman image and secret is embedded into the watermarked image.
Fig 5: Retrieval of image and the data.

The process of extracting the watermarked image to get the hidden data is carried out through the following steps,

Step 1: The received image which contain the hidden part to be extracted.
Step 2: In the received image extract the watermarked part separately using inverse DWT process.
Step 3: In the watermarked content give the secret key which is given in the embedding side and the watermark image is taken.
Step 4: In the watermark image, the data is taken through by applying the inverse DWT process.
Step 5: Finally the image and the data are taken in the receiver side.

The MSE values are given as,

\[ MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} |I(i, j) - J(i, j)| \]  

(3)

The calculation of PSNR values are processed through,

\[ PSNR = 20 \log_{10}(\text{MAX}_i) - 10 \log_{10}(\text{MSE}) \]  

(4)

\[ \text{MAX}_i \] are represented as \(2^n-1\) bits sample per second.

The PSNR, MSE and time taken by the processing of embedding and extraction of image during the process are calculated using some mathematical expressions. Then the values are tabulated below for the process,

<table>
<thead>
<tr>
<th>Lena Image</th>
<th>png</th>
<th>bmp 24 CB</th>
<th>jpeg</th>
<th>bmp 16CB</th>
<th>gif</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR(dB)</td>
<td>13.0288</td>
<td>9.2336</td>
<td>13.0284</td>
<td>9.2333</td>
<td>12.6722</td>
</tr>
<tr>
<td>MSE</td>
<td>56.8987</td>
<td>88.0767</td>
<td>56.8984</td>
<td>88.0800</td>
<td>59.2328</td>
</tr>
<tr>
<td>Time to Embed the data into an image(s)</td>
<td>36.5268</td>
<td>39.5214</td>
<td>30.2700</td>
<td>36.1967</td>
<td>38.030758</td>
</tr>
<tr>
<td>Time Extraction(s)</td>
<td>76.2451</td>
<td>52.6347</td>
<td>82.0324</td>
<td>55.1482</td>
<td>51.928742</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Camera man image</th>
<th>png</th>
<th>bmp 24 CB</th>
<th>jpeg</th>
<th>bmp 16CB</th>
<th>gif</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR(dB)</td>
<td>10.7340</td>
<td>12.4194</td>
<td>9.8104</td>
<td>14.2895</td>
<td>12.1755</td>
</tr>
<tr>
<td>MSE</td>
<td>67.2199</td>
<td>74.2061</td>
<td>55.9822</td>
<td>62.4194</td>
<td>83.8861</td>
</tr>
<tr>
<td>Time to Embed the data into an image(s)</td>
<td>40.6510</td>
<td>32.7841</td>
<td>37.3977</td>
<td>44.8261</td>
<td>38.0187</td>
</tr>
<tr>
<td>Time Extraction(s)</td>
<td>52.8174</td>
<td>57.3920</td>
<td>47.2896</td>
<td>73.0918</td>
<td>63.1574</td>
</tr>
</tbody>
</table>

Conclusion:

The proposed measure is simply the logarithmic scale of the probability of reaching this goal. This is similar to the brute force attack in cryptography, with the notable difference that there might not be a unique key granting the access to the watermarking channel. Not only using DWT process but also different kinds of wavelet transform are used. Then different watermarking technique are used through the same Effective Key Length and by varying the parameters. For the replacement of data some other content like scanned copy, question paper etc..., for transmission in secure manner. The future work is to minimize the key length for small \(N_0\).
REFERENCES


