DATA HIDING FOR BINARY IMAGE BY CONNECTIVITY-PRESERVING

A. R. CHANDEKAR

M.E.(E &TC) Student, MITCOE, Pune, Maharashtra, India

ABSTRACT

Digital watermarking and data hiding techniques are used in many applications such as ownership protection, copy control, annotation, and authentication. In this method of blind data hiding for binary image by preserving the connectivity among pixels in a local neighborhood. Embedding the data in binary image is possible by flipping the pixels. The flippability decision of a pixel depends on three transitions from the pixels to its eight neighbors in a 3X3 block. Flipping a pixel does not destroy the connectivity among pixel, to ensure the good visual quality of an image. Fixed Block method of partitioning an image is discussed here. Security issue, visual quality, various methods of data hiding are discussed.

KEYWORDS: Binary Image, Connectivity Preserving, Data Hiding

INTRODUCTION

Digital watermarking is a technique of inserting information into an image, which can be extracted or detected for identification and authentication purposes. There are different types of watermarks are designed for different applications. For example, ownership assertion images that are to be made publicly available, so that unauthorized users who claim ownership or resell the images without the permission of the original owner can be held accountable. Such watermarks are robust, that the watermark is usually detectable even after the watermarked image has been processed by image processing algorithms like scaling, cropping and compression. Data hiding and watermarking in greyscale or color image is easier because the pixels has a wide range of values, slight change in the pixel value does not cause any visually noticeable change in the image. Besides that in the binary image it consist either “0” or “1”. Flipping pixels randomly in the non edge region will create noticeable change in the image.

The main focus is on data hiding in a binary image for image authentication. using “Connectivity preserving” criterion. To check the “flippability” of a pixel. The criterion is based on the connectivity among pixels; it plays an important role to the visual qualities. The visual quality is ensured, if flipping a pixel does not destroy the connectivity among pixels. The location of the “embeddable” pixels is discussed, and an authentication scheme is designed to make the cryptographic signature to ensure the authenticity and integrity of the image.

The main objectives are as follows:

- Check the “flippability” of a pixel using the “connectivity preserving” criterion to get good visual quality of the watermarked image.
- An “uneven embeddability” of the image for embedding the watermark only in the“embeddable”blocks.
- Study the features of flipping pixels in binary images to Achieve blind watermark extraction
- Investigation on how to locate the “embeddable” pixels in the watermarked image to get cryptographic signature to achieve higher security.
LITERATURE SURVEY

Watermarking and data hiding techniques can be classified according to the embedding methods: text line, word, or character shifting, boundary modifications, fixed partitioning of the image into blocks, modification of character features, modification of run-length patterns, or modifications of half-tone images. In the method of shifting a text line, a group of words, or a group of characters or modifying the feature of character by a small amount to embed data is proposed in [3]-[8]. These methods are applicable to documents with formatted text. These methods are applicable to documents containing the paragraphs of printed text. Data is embedded in text documents by shifting lines and words spacing by a small amount (1/150 inch.) A text line can moved up or down to encode a ‘0’, a word can be moved left to encode a ‘1’ or right to encode ‘0’. The techniques are useful for printing, photocopying, and scanning. In the decoding process, distortions and noise introduced by printing, photocopying and scanning are removed. The capacities of these methods are low. The method of partitioning an image into fixed blocks of size m x n, and computes pixel statistics from the blocks for embedding data, are proposed in [9], [10]. These methods are applicable for binary document images egdocument with formatted text or engineering drawing. The input image is partitioned into blocks and a fixed number of bits are embedded in each block. The flipping priority of a pixel is indicative measure for visual distortion that would be caused by flipping the value of a pixel from 0 to 1 or from 1 to 0. Smoothness of image is measured by the horizontal, vertical, and diagonal transitions, and connectivity is measured by the number of black and white pixels in the 3 x 3 window. Data is embedded in a block by modifying the total number of black pixels to be either odd or even, representing data bits 1 and 0, respectively. It is done by random permutation of all pixels in the image after identifying the flappable pixels. In [11], a data hiding technique using a secret key matrix K and a weight matrix W is used to protect the hidden data in a binary image. This method does not provide good visual quality in the watermarked document. In boundary modifications technique [12], the data is embedded in the 8-connected boundary of a character. A fixed set of pairs of five-pixel long boundary patterns is used to embed data. One of the patterns in a pair requires deletion of the center pixel, whereas the other requires the addition of a foreground pixel. A unique property of the proposed method is that the two patterns in each pair are dual of each other changing the pixel value of one pattern at the center position would result in the other. This property allows easy detection of the embedded data without referring to the original document, and without using any special techniques for detecting embedded data. The method can be applied to general document images with connected components e.g. text documents or engineering drawings. In the modifications of character features techniques, modification is made in the character features to embed data. In [13], text areas in an image are identified first by connected component analysis, and are grouped according to closeness. Each group has a bounding box that is divided into four partitions. The four partitions are divided into two sets. The average width of the horizontal strokes of characters is computed as feature. To compute average stroke width, vertical black runs with lengths less than a threshold are selected and averaged. Two operations “make fat” and “make thin” are defined by increasing and decreasing the lengths of the selected runs, respectively. To embed a “1” bit, the “make fat” operation is applied to partitions belonging to set 1, and the “make thin” operation is applied to partitions belongs to set 2. The opposite operations are used to embed “0” bit. In the detection process, detection of text line bounding boxes, partitioning, and grouping are performed. The stroke width features are extracted from the partitions, and added to set. If the difference of the sum totals is larger than a positive threshold, the detection process outputs 1. If the difference is less than a negative threshold, it outputs 0. This method could survive the distortions caused by print-and-scan (re-digitization) processes. In the Modification of Run-Depths [14], a method was proposed to embed data in the run-lengths. A document contains 1,728 pixels in each horizontal scan line. Each run length of black (or foreground) pixels is coded using modified Huffman coding technique according to the statistical distribution of run-lengths. Each run length of black pixels is shortened or lengthened by one pixel according to a
sequence of signature bits. The signature bits are embedded at the boundary of the run lengths according to some pre-defined rule. In the modifications of Half-Toning Images is a watermarking techniques are used for half-tone images that can be generally found in printed matters such as books, magazines, newspapers, printer outputs, etc. This types of methods are only useful for half-tone images, and are not suitable for other types of document images is proposed in [15]. The work of hiding data in binary image are discussed in [16], [17].

In the proposed method the connectivity-preserving criterion is used to hide the data in a 3X3 neighborhood of pixel. The “uneven embeddability” is used for embedding the watermark in only “embeddable” blocks. The problem of location of the “embeddable” pixels and the extraction the watermark are discussed. The proposed method of watermarking can be applied for text documents, cartoon, engineering drawing, handwritten signatures and even halftone images authentication.

**IMPLEMENTATION SCHEME**

**Flippability Decision**

In the 4-connectivity and 8-connectivity among pixels, the flippability decision of a pixel depends on the transitions of the pixel to its eight neighbors in a 3X3 block. The eight neighbors of the center pixel ‘Pc’ in a 3X3 neighborhood are \(\omega_1, \omega_2, \omega_3, \omega_4, \omega_5, \omega_6, \omega_7, \) and \(\omega_9\), shown in Figure 1, where \((i, j)\) denotes the pixel located at ‘i’ th row and ‘j’ th column of the image. Use “1” and “0” to denote black and white pixels, respectively.

**Case 1:** The uniform white transition and the uniform black transitions in a 3X3 block along vertical and horizontal directions are collectively defined as “VH Transition” and given by

\[
N_{VW} = \sum_{k=1}^{3} P_c \cdot \omega'_k \cdot \omega'_{K+4}, \quad N_{VB} = \sum_{k=1}^{3} P_c \cdot \omega_k \cdot \omega'_{K+4}
\]

(1)

Where \(\omega'\) denotes logically “Not \(\omega\)” and “\(\cdot\)” is the logical “And” operation for binary data.

**Case 2:** The number of the interior right angle transitions in a 3X3 block is defined as “IR Transition” and is given by

\[
N_{ir} = \sum_{k=1}^{4} P'_c \cdot \omega_{2k+1} \cdot \omega'_{2k-1}
\]

(2)

Where, \(\omega_{2k+1} = \omega_{1}, \) for \(2k+1 > 8\)

**Case 3:** The number of transitions from the center pixel to the sharp corners in a 3X3 block is defined as “C Transition” is and given by

\[
N_{C} = \sum_{k=1}^{4} P_c \cdot \omega_{2k+1} \cdot \omega_{2k+2} \cdot \omega_{2k+3} \cdot \omega_{2k+4}
\]

(3)

Where, \(\omega_{9} = \omega_{1}, \omega_{10} = \omega_{2}, \omega_{11} = \omega_{3}\) and \(\omega_{12} = \omega_{4}.

The “Flippability Criterion” is defined in such a way that the center pixel in a 3X3 block is “flippable” if the number of VH transition \(N_{VW}\) and \(N_{VB}\), the number of IR transition and the number of transition \(N_{ir}\) and the number of C transition \(N_c\) remain the same before and after flipping the center pixel.

If the transition numbers do not change, then it clear that flipping the pixel will not destroy the connectivity among pixels in the neighborhood and also does not create any distortion. Where as \(N_c\) is used to control the flippability of
pixels in sharp corners so that the 8-connectivity among pixels is not destroyed. This criterion is known as “Connectivity-Preserving” criterion.

The reason of the connectivity preserving among pixels in 3X3 neighborhoods can be explained as follows.

The pixels that meet the condition in (1) would have two white 4-neighbors, so, it is a boundary pixel as shown in Figure 2(a). The condition (2) is to ensure that flipping the center pixel does not create any cluster. The isolated corner pixel is the corner pixel that has three white neighbors in a 3X3 block as shown in Figure 2(b), by satisfying the conditions (1) and (2), at least one corner has three white pixels. It is further ensures that flipping the center pixel will not destroy the connectivity of the pixel pattern. Finally, by meeting the conditions in (3), it implies that flipping the center pixel will not destroy the 8-connectivity of the center pixel and its neighbors. Therefore it satisfying the “Connectivity-Preserving” criterion.

**Block Partition and Embeddability**

The Partitioning of an image in different ways, to get the different types of blocks for the data hiding process. In propose method the fixed block of size 3X3, image of size 6X6 is partitioned into four 3X3 blocks (FB), non-interlaced block (NIB), image of size 8X8 is partitioned into four non-interlaced 4X4 and in interlaced block (IB), image of size 7X7 is partitioned into four interlaced 4X4 block schemes. For the interlaced block scheme, any two vertically or horizontally neighboring blocks share one common row or column that are not used in the data hiding process. The “embeddability” of a block depends on the “flippability” of the determined pixels in the block, the determined pixels are the center pixels of the blocks for the fixed 3 X 3 block scheme, all pixels except the boundary pixels for the non-interlaced block scheme and all pixels except those lie in the sharing rows and columns for the interlaced block scheme.

<table>
<thead>
<tr>
<th>(i-1,j-1)</th>
<th>(i,j)</th>
<th>(i-1,j+1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>W6</td>
<td>W7</td>
<td>W8</td>
</tr>
<tr>
<td>(i,j-1)</td>
<td>P_c</td>
<td>(i,j+1)</td>
</tr>
<tr>
<td>W5</td>
<td>W1</td>
<td>W2</td>
</tr>
<tr>
<td>(i+1,j-1)</td>
<td>(i+1,j)</td>
<td>(i+1,j+1)</td>
</tr>
<tr>
<td>W4</td>
<td>W3</td>
<td>W2</td>
</tr>
</tbody>
</table>

**Figure 1: Designation of Pixels in 3*3 Neighborhood**

![Figure 2: The 3 X 3 Block Patterns](image)

(a) Satisfy VH Transition, (b) Satisfy VH Transition and C Transition but do not Satisfy IR Transition, and (c) Satisfy VH Transition and IR Transition but do not Satisfy C Transition

**Watermark Embedding and Extraction**

The watermark embedding process consists of following steps.

- Partition the input image into equal size square blocks.
- According to “Flippability Criterion”, check the flippability of the pixels.
- Identified the “flippable” pixel, the block is marked as “embeddable”. The “flippable” pixel is identified as the “embeddable” pixel.
- Apply step 1 to 3 for next block.
- In this way process the complete image.
- Embed the watermark (image to be hide) in the “embeddable” blocks. By flipping the “embeddable” pixels (if needed) to enforce the odd-even feature of the number of black or white pixels in the block.

The watermark extraction and verification process is as below:

- Find the “embeddable” locations, generate the intermediate image and generate the hash value of the watermarked image it is similar to steps 1 to 3 in the embedding process.

**Figure 3: Block Diagram of the Hard Authenticator Watermark Embedding Process**

**Figure 4: Block Diagram of the Hard Authenticator Watermark Verification Process**

- Extract the watermark based on the odd-even feature of the number of black or white pixels in the “embeddable” blocks.
- Employ the private key to decrypt to obtain the hash value of the original image.
- Compare it with original watermark image. The match is found same, the authenticity and integrity of the image can be ensured.
Flow Charts

1. Capacity Calculation

Start

Divide image into 3x3 blocks

Capacity for each block

Apply flexibility criterion

Criteria satisfy capacity

Total Capacity

2. Data Hiding

Start

Get Data

Convert Data into binary

Divide image into 3x3 Block

Apply flexibility criterion for each block

Flip center pixel, again apply criterion

Is pixel flexible

Y

Embed current bit into center pixel

N

3. Data Extraction

Start

Divide Watermark image into 3x3

Check center pixel of each block

Compare it with center pixel

Change in center pixel

Y

Extract Data

N

EXPERIMENTAL RESULTS

Various images are used to test the capacities of data embedding using fixed partitioning of images. The results are shown in TABLE 1. It can be seen from table that the complete black, complete white image and black and white image has embedding capacity is -1. Again the images with sharp corner has zero embedding capacities. Other images where there is a shade of black and white have more capacity to embed the data.

Images taken are of different pixel values and the criterion is applied for the images such as black, black and white, text, cartoon, and other many images to find the capacity for hiding data. Then in the next stage data which has to be hide is entered. After hiding data the image displayed, there is no change occur in the image. It means that image integrity is achieved. After that hidden data is extracted from the image by applying the criterion.
**Applications**

The proposed authentication system can be applied for digital document authentication such as digital certificate (e-Certificate). It can be also applied for text document, cartoon, engineering Drawing, handwritten signatures and even half tone images authentication.

**CONCLUSIONS**

- In this method of data hiding in binary images authentication based on connectivity-preserving criterion of pixels in a local neighborhood is presented. A window of size 3* 3 is used to assess the “flippability” of a pixel in a block.

- An “uneven embeddability” of the host binary image is handled by embedding the watermark in only “embeddable” blocks based on the three transition criteria.

- An “uneven embeddability” of the host binary image is handled by embedding the watermark in only “embeddable” blocks based on the three transition criteria.

- The fixed 3X3 fixed block studied.

- The problem of location of the “embeddable” pixels in a block for different block method is addressed.

- A proposed scheme is applied to wide variety of image authentication.

---

**Table 1: Capacity Comparison of Different Images**

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Name of Image</th>
<th>Size(Px)</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Text</td>
<td>486*533</td>
<td>97</td>
</tr>
<tr>
<td>2.</td>
<td>Cartoon</td>
<td>157*153</td>
<td>10</td>
</tr>
<tr>
<td>3.</td>
<td>Black</td>
<td>201*201</td>
<td>-1</td>
</tr>
<tr>
<td>4.</td>
<td>Black&amp; white</td>
<td>201*201</td>
<td>-1</td>
</tr>
<tr>
<td>5.</td>
<td>Winter</td>
<td>390*340</td>
<td>81</td>
</tr>
<tr>
<td>6.</td>
<td>Hill</td>
<td>390*314</td>
<td>5</td>
</tr>
<tr>
<td>7.</td>
<td>Sunset</td>
<td>427*302</td>
<td>45</td>
</tr>
<tr>
<td>8.</td>
<td>Water</td>
<td>390*327</td>
<td>137</td>
</tr>
</tbody>
</table>
REFERENCES


