Data Hiding for Text Document Authentication by Connectivity Preserving

S.P. Kamalapriya and R. Ramesh

Abstract--- In this paper, a novel blind data hiding method for text document images aims to preserve the connectivity in a local neighbourhood is proposed. The "flippability" of a pixel is determined by imposing the three transition criterions in a 3x 3 moving window which is centered at the pixel.the "embeddability "of a block is invariant in the watermark embedding process. While the "flipped "pixels can be located by imposing a constraint. The uneven "embeddability" of the host image is considered by embedding the watermark only in those "embeddable" blocks. The location is chosen in such a way that the visual quality of the watermarked image is guaranteed. Different types of blocks are employed and their abilities to increase the capacity are compared. A hard authenticator watermark is also generated tom ensure the integrity and authenticity of the document.

I. INTRODUCTION

Authentication of digital documents has aroused great interest due to the wide application area nowadays, e.g. bank checks, legal documents, certificates, digital books and maps. Very often, digital documents are stored in binary format. Since digital documents are easy to copy and edit via the software tools, authentication and detection of tampering is of utmost concern.

In the past few years, a limited number of papers proposed new techniques for document watermarking and data hiding. Among these techniques, some results in noisy watermarked image due to the weak quality control e.g. the key-weight matrix based method. Some require a shuffling key in order to distribute the "flibbable" pixels all over the image. It may be difficult to find a proper shuffle key such that in each block of the shuffled image there is a suitable pixel to flip. Therefore, a larger block size, e.g. 12x12 Is required.

In this paper, we propose a data hiding technique, which is based on the connectivity –preserving in 3x3 neighborhood. The "uneven embeddability "of the host image is considered by embedding the watermark only in those "embeddable" blocks. A small block size, e.g. 4x4 is employed in order to achieve the larger capacity. The proposed scheme can be used for document authentication. E.g. eCertificate authentication.

II. PROPOSED METHOD

The flippability of a pixel depends on the transitions from the pixel to its eight neighbors in a 3x3 block. The 8 neighbors of the center pixel p (i,j) are denoted as N(p) and shown as

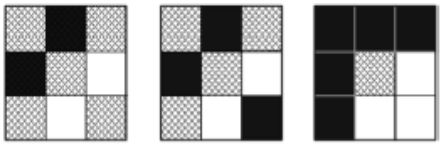

Fig. 1: Designations of Pixels in 3x3 Neighbourhood

Let's define "1" represents the black pixel and "0" represents the white pixel.

S.P. Kamalapriya, M.E, Lecturer, Dept of CSE, K.Ramakrishnan College of Engineering, Trichy. E-mail:kamalapriya12@gmail.com
R. Ramesh, M.E, Assistant Professor, Dept of CSE, K.Ramakrishnan College of Engineering, Trichy. E-mail:rameshcsekrce@gmail.com

Definition1

The number of uniform white and black transitions in a 3x3 block along the vertical and horizontal directions is named as "VH Transition", denoted as NVHW and **N** VHB and defined as

$$N_{VHW} = \sum_{i=1,3} p.\overline{w}_i\overline{w}_{i+4} \text{ and } N_{VHB} = \sum_{i=1,3} p\, w_{Iw\,i+4}$$

Where, w implies logically "not w"

Definition 2

The number of transitions of the interior right angle is named as "I R Transitions" and denoted as **N**IR.

$$\mathbf{N}IR = \sum p\,\overline{w}\,2i\ \overline{w}\ 2i - 1.\overline{w}2i + 1$$

Where, $\overline{w}2i + 1 = w1, for\ 2i + 1 > 8.$

Definition 3

The number of transitions from the center pixel to the sharp corners in a 3x3 block is name das "C Transitions " denoted as Nc and defined as

$$Nc = \sum_{i=1}^{4} pw2i.w2i+1.w2i+2.w2i+3.w2i+4$$

Where w9=w1, w10=w2, w11=w3, w12=w4

Definition 4

"Flippabilityy Criterion", the center pixel in a 3x3 block is "flappable" if the number of VH transition, NVHW and NVHB and the number of sharp corner transition Nc remain the same before an dafter flipping the center pixel.

NVHW, NVHB and NIR are calculated before and after flipping the center pixel.

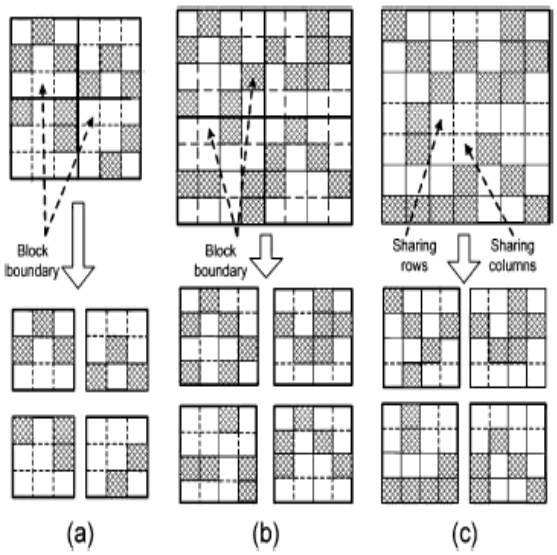

Fig. 3. Illustration of (a) fixed 3 × 3 block, the image of size 6 × 6 is partitioned into four 3 × 3 blocks, (b) non-interlaced block, the image of size 8 × 8 is partitioned into four non-interlaced 4 × 4 blocks, and (c) interlaced block, the image of size 7 × 7 is partitioned into four interlaced 4 × 4 blocks.

If the transition does 't change, it implies that flipping the pixel won't destroy the connectivity between pixels in the neighbourhood and doesn't create extra clusters a well. These two conditions are collectively named as "Connectivity Preserving "criterion. While Nc is used to control not to flip pixels in sharp corners, as it is annoying to human observers. The qualified blocks which satisfy the "V H Transition ", excluded by the "I R Transition ' and: C Transition".

The pixels meet the condition defined in (1) would have two white 4-neighbours, so it is a boundary pixel. The condition defined in (2) is to ensure that flipping the center pixel doesn't create an isolated pixel (a pixel has eight white neighbors). Furthermore, by satisfying conditions define drain (1) and (2), at least one corner has three white pixels. This further ensures that flipping the center pixel won't destroy the local connectivity of the pattern.

A. Block Partition and Embeddability

Different types of blocks are employed. They are: fixed 3x3 block (FB), non interlaced block (NIB) and interlaced block, any two vertically or horizontally neighboring block share a common row or column.

B. Capacities

Let's assume the probability that a pixel satisfies the three conditions is: P, then the probability of each block to be "embeddable" is 1/9 p for a fixed 3x3 block;

((n-2)x(n=2)/nxn)p for a non interlaced block with block size nxn; and ((n-2)x(n-2)/nxn)p for an interlaced block with block size nxn .The total block number is:[W/3]x[H/3] for a fixed 3x3 block; :[W/n]x[H/n] for a non interlaced block;

[W/(n-1)] x [H/(n-1)] for interlaced block; where W, H are the width and height of the image, while [x] is the floor function which gives the largest integer less than or equal to x.

It is obvious that the total block number has increased for the interlaced block compared with the non-interlaced block. More pixels can be flipped by using moving window to increase the probability that a block to be "embeddable". However, the total block number will be decreased.

C. Watermark Embedding and Extraction

- The watermark embedding process is summarized as follows:
- Partition the image into equal size square blocks.
- Determine flippability of the determined pixels based on the: Flippability Criterion.
- Once a pixel is identified as "flappable", the block is marked as "embeddable"
- Proceed to the next block.
- Repeat steps 2 to 4 until all blocks are processed.
- Embed the watermark in the "embeddable" blocks by enforcing the odd-even features of the number of black or white pixel in the block.

Lemma1

The "embeddability" of a block is invariant in the watermark embedding process.

Proof

From the "Flippability Criterion ", the "flippability" of a pixel is invariant in the embedding process. So a "flappable" pixel is still "flappable" and an "embeddable" block remains "embeddable".

Let's divide the pixels in the *K*th "embeddable" block {p} into two sets: determined pixels Dk € {A} and the non-determined pixels Uk € {B}. Assume the first "flappable" pixel in the Kth block is Pk, *Fpk*=1,since the "flippability" of a pixel is invariant, so,Fpk' =Fpk=1.the "embeddability" of the block is:Sk=Fpk=1.Flip Pk will affect the flippability of its eight neighbours,Fqk,qk € {N{p}}.However since Uk won't be flipped,qk may be located farthest at the boundary;i.e qk € {B},qk € { A } U { B }={ P} therefore, *qk* is still in the same block,thus,flipping a pixel in one block doesn't affect the "flippability " of pixels in its neighboring blocks. The "embeddability" Of this block is: $S_k'=f_{pk}$ V f_{dk} ' V…=1, if q_k ε {A} and fqk'=1. Otherwise, $S_k'=f_{pk}'=1$. Hence, the "embeddability" of the block is invariant. The watermark can be extracted blindly from the "embeddable" by computing the odd-even feature of the number of black or white pixels.

III. THE AUTHENTICATION MECHANISM

The odd-even enforcement is employed for the watermark embedding, which is vulnerable to "parity attack", i.e., an adversary can carefully flip two pixels while keeping the odd-even feature of the block unchanged. So, we propose to adopt a hard authenticator watermark to tackle this problem.

A. Locate Flipped Pixels

In order to generate the hard authenticator watermark, the key issue is how to locate the flipped pixel given the watermarked image. For the fixed 3 x 3 block, the flipped location is always the center pixel of the block; therefore it is easy to locate the flipped pixel.

Lemma 2

For non-interlaced block, if flipping the current pixel does not change the "flippability:" of its previous four neighbors in the same 3 x 3 window, the flipped pixel can be located.

Proof

Pixels in the 3x3 block (fig.1) are processed in row-by-row and column-by-column sequence, i.e., w6, w7, w8, w5, p, w1, w4, w3 and w2. Assume p is the first "flippable" pixel in the block, i.e., fw6=fw7=fw8=fw5=0 and fp=1. Given the condition, i.e., flip pixel p won't change the "flippability" of its previous four neighbors, we get fw6'=fw7'=fw8'=fw5'=0. Since the flipability of a pixel is invariant, so, fp'=fp=1. During the watermark extraction, pixels in the block are processed in the same sequence. Hence, the "flipped " pixel p can be located. The boundary pixels are excluded from flipping renders the minimum distance between any two "determined" pixels in two neighboring block is 2. There fore, changes in pixels in one block won't affect the "flippability" of pixels in its neighboring block.

While for the interlaced block, flip p may affect one of the transition numbers of its previous four neighbors {p4}. If {p4} lie in the sharing row or column, they may again be the previous four neighbors of pixels, e.g., m, n will be processed prior to pixel p. So, it may change the "embeddability" of its previous block. Therefore, the flipped locations cannot be located by setting the same constraint. In this case, we suggest apply shuffling to the original image or to the "embeddable" "unembeddable" blocks to increase the system security.

B. The Authentication Process

Fixed 3x3 block and non-interlaced block are employed in the hard authenticator watermark embedding process, which is summarized below and shown in Fig.4.

- Find the "embeddable" locations based on the steps S1-S5 discussed in 2.4. Criterions for locating the pixels are also imposed.
- Similar to clear LSB for grayscale images[3], clear the "embeddable" location by setting it to a fixed value, e.g., "0" to generate the intermediate image Y1.
- Fed Y1 into a hash function to generate the hash value, Ho=Hash (Y1).
- Encrypt the Ho by the private key Ks of the owner or issuer, e.g., RSA private key to generate the content signature of the document, Ws=Ek(H0,Ks).
- XOR (Exclusive OR) or concatenate Ws with the payload watermark Wp to generate the authenticator watermark, e.g., Wr=Ws || Wp.
- Embed Wr in the "embeddable" blocks based on the odd-even feature of the block.

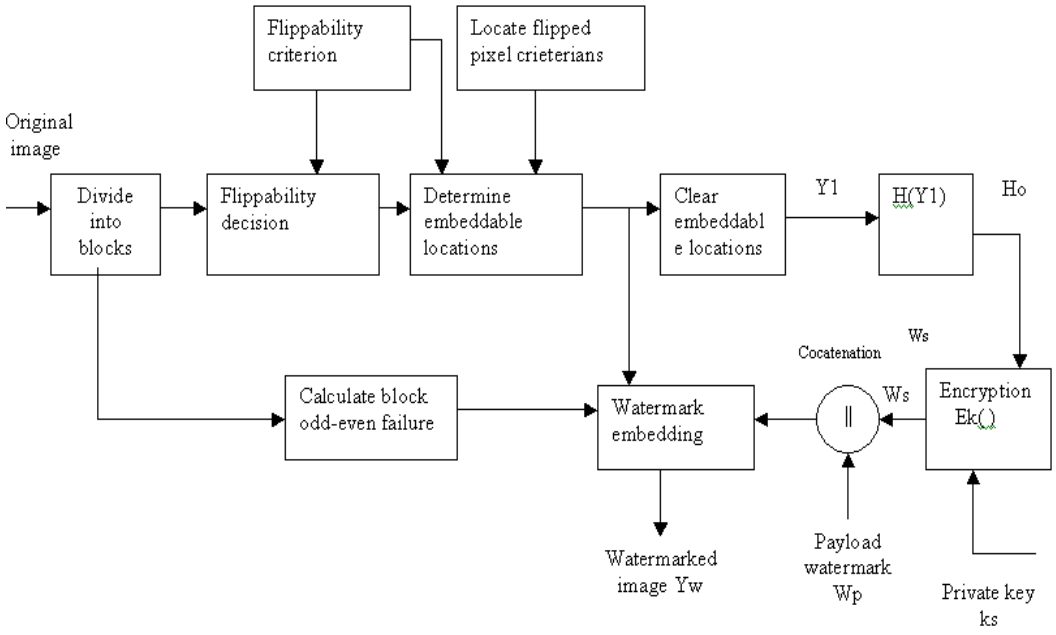

Fig. 4: Block Diagram of Hard Authenticator Watermark Embedding Process

C. The Verification Process

The hard authenticator watermark verification process are summarized below and shown in Fig.5.

1. The first three steps, i.e., find the "embeddable" locations, generate the intermediate image Y1' and generate hash of the watermarked image Hw are the same as steps 1-3 in the embedding process.
2. Extract the watermark based on the odd-even feature of the "embeddable" block, split it into two parts: the content signature Ws' and the payload Wp'.
3. Employ the public key Kp, e.g., RSA public key to decrypt Ws', e.g., the first 1024 bits to obtain the hash value of the original image Ho'=Dk (Ws', Kp).
4. Compare Wp' with Wp and Hw with Ho'. If Ho' match Hw and Wp' is the same as Wp, the authenticity and integrity of the document can be ensured.

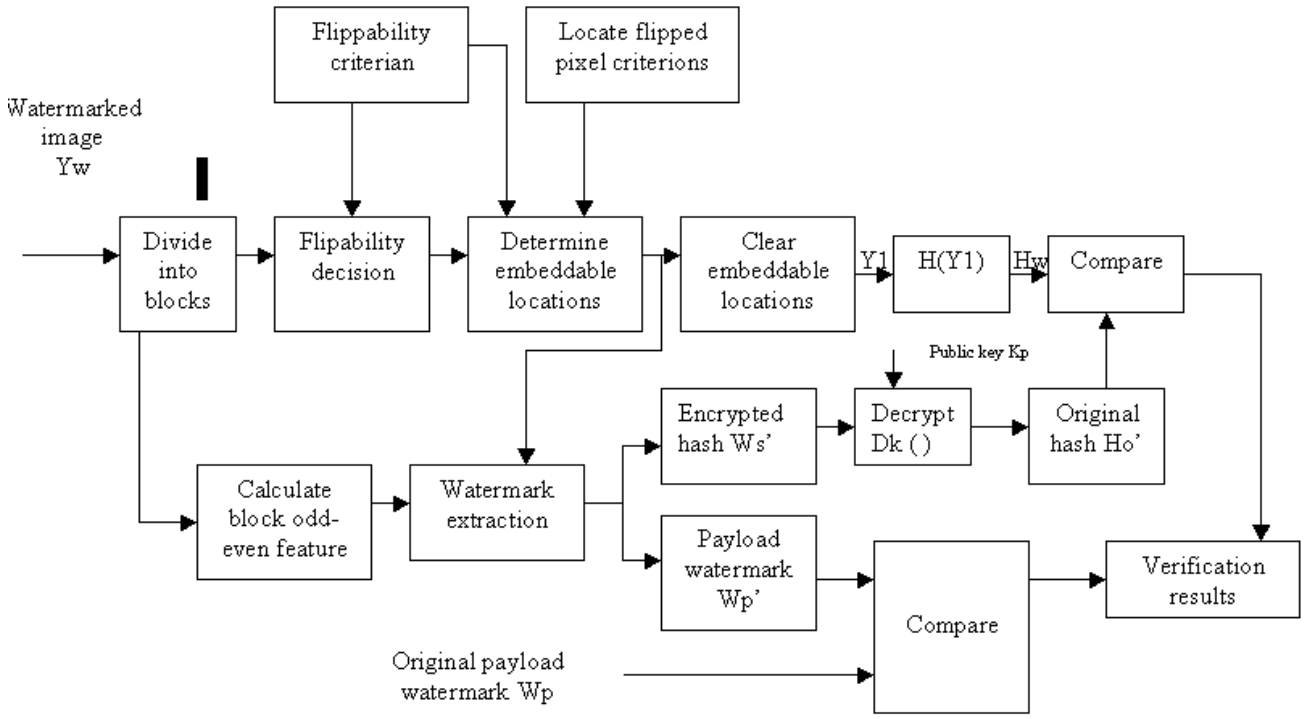

Fig. 5: Block Diagram of Hard Authenticator Watermark Verification Process

IV. EXPERIMENTAL RESULTS

A wide range of images, including cartoon images, English, French, Chinese and handwritten text images are used to test the capacities of using different types of blocks. The results are shown in the Table 1. It can be seen from the results, by employing the non-interlaced block of size 4 x 4, the capacity increases compared with a fixed 3 x 3 block. By employing interlaced block of size 3 x 3, the capacity increases further.

File	Size	Capacity (bits)			
		1) FB 3 X 3	2) NIB 4 X 4	IB 3) 3 X 3	IB 4 X 4
Fre	512 X 512	1795	2448	3383	4389
Gir	361 X 359	248	261	396	478
Chi	336 X 336	482	733	1052	1261
Typ	336 X 336	447	672	1006	1235
Han	336 X 336	313	454	741	972
Jap	336 X 336	526	822	1180	1488

Experimentally, the use of interlaced block with size 4 x 4 gives the largest capacity. Experiments are also conducted to verify the effectiveness of the proposed hard authenticator watermark. A logo image is used as the payload watermark to visually show the tamper occurred to the watermarked image. The results are shown in Fig. 6. It can be of the author's watermark; coefficient and quantization selection keys (which we describe later) and the quantization parameter Δ are necessary to embed and to extract the mark. The watermark can be an encrypted version of the author identification, which is

Fig. 6: The Reconstructed Logo Image (No Tamper) and the Reconstructed Logo Image (Tampered).

Observed from the results that the proposed hard authenticator watermark is effective in detecting any tampering made to the watermarked document. The logo image can be reconstructed successfully when no tampering occurs. However, when tamper occurs, even the tamper is small, e.g., only one word is shifted slightly, the computed hash varies significantly.

V. CONCLUSION

In this paper, a novel blind data hiding scheme for binary images based on connectivity preserving of pixels in a local neighborhood is presented. A window of size 3 x 3 is employed to Asses the “flippability” of a pixel in a block. Watermark is only embedded in those “embeddable” blocks based on the three transition criterions. The fixed 3 x 3 block, non-interlaced and interlaced block are employed and the capacities of using different types of blocks are compared. Experimentally, it is shown that the interlaced block with size 4 x 4 gives the largest capacity. A hard sauthenticator watermark is employed which is effective in detecting any tampering to the watermarked image.

REFERENCES

[1] Y.C.Tseng and HK.Pan, “data hiding in two color images”IEEE Transactions on Computers.
[2] A. Frome, Y. Singer, F. Sha, and J. Malik, “Learning globally-consistent local distance functions for shape-based image retrieval and classification,”in Proc. Int. Conf. Comput. Vis., 2007, pp. 1–8.
[3] Z. Jiang, Z. Lin, and L. S. Davis, “Learning a discriminative dictionary for sparse coding via label consistent -SVD,” in Proc. Comput. Vis.Pattern Recognit., 2011, pp. 1697–1704