International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

Advance Digital Watermarking

Utkarsha B. Badhan[1], **Prashant R Kotkar**[2]
[1]*Department of Computer Engineering, S.N.J.B's KBJ COE, Chandwad, utkarshabadhan@gmail.com*
[2]*Department of Chemical & Paper Engineering, Western Michigan University, Kalamazoo (MI), USA, kotkarprashant@gmail.com*

Abstract— The advent of the Internet has resulted in many new opportunities for creating and delivering content in digital form. Applications where digital watermarking is used are copyright protection, source tracking (different recipients get differently watermarked content), broadcast monitoring (television news often contains watermarked video from international agencies), video authentication and web publishing. An important issue that arises in these applications is protection of the rights of document owners. It has been recognized for quite some time that current copyright laws are inadequate for dealing with digital data. This has led to an interest in developing new copy deterrence and protective mechanisms. Digital watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes, including copy prevention and control. We will be using LSBs of Blue components to rearrange the data in the original image so that it will give us very less distortion in the range of 0.00001 percent, which is not detectable by the human naked eyes. And thus we will embed our watermark information. We are making use of blue component of pixel as it has the LSB of the value and changing the LSB will affect the least to the value.

Keywords- Digital watermark, LSB bit, Robust

I. INTRODUCTION

The explosive growth of Internet and communication networks has led to the tremendous use of multimedia data like image, audio and video. Furthermore, due to the availability of tools to manipulate digital multimedia especially digital images, data can be easily tampered. It is important to ensure the integrity and protection against unauthorized duplication of images and videos. A common technique is digital watermarking, a process by which a user-specified signal (watermark) is hidden or embedded into another signal, for example digital content such as electronic documents, images, sounds and video.

1.1 Image watermarking:

In this scheme, a binary logo image is used as the original watermark W of size pixels 32*32, which is shown in Fig. 1.1(a). In order to construct a good watermark for embedding, the original watermark is permuted to obtain a pseudo random sequence, which uncorrelated to the original watermark as shown in Fig.1.1 (b). This is done by performing bit wise EX-OR operation between the original watermark bits and random bits, which generated using a secret key and then the output sequence, is encoded using gray code. The permutation process of the watermark W is described as follows:

$W = \{W(i, j), 1 \le i \le 32, 1 \le j \le 32, w(i, j) \in (0,1)\}$

K is the chaotic binary sequence, which is the secret key

$K = \{k(i, j), i \le 1 \le 32, 1 \le j \le 32, k(i, j) \in (0,1)\}$

$W' = W \oplus K$ where $\oplus$ denotes XOR operation.

The permuted watermark *W″* is obtained by applying Gray code to *W′*

Fig 1.1(a): Original Watermark

Fig 1.1(b): Permuted Watermark

1.1.1 Watermark embedding

The proposed watermark-embedding scheme is shown in Fig.1.1.1 In the proposed method; the watermark image is a binary image where as the host image is an 8-bit color image. The watermark is embedded four times as shown in Fig1.1.2 in different positions. The four embedded positions are chosen to hide the watermarks in order to be robust against cropping attack from the bottom, the top or the left or the right side of the watermarked image. The blue component is chosen to hide the watermark because it is less sensitive to human eyes. Suppose the original color image H with size of 512*512 pixels, which to be protected by the binary watermark W of size pixels 32*32, the original image H is divided into a non-overlapping blocks of 8*8 and each bit of the encoded watermark is embedded in a block, therefore one watermark is required 1024 blocks.

The embedding process is described as follows:

Step 1: The watermark W is permuted.

Step 2: The original image H is decomposed into R, G, and B components and then the B component is divided into a non-overlapping blocks with size of 8*8 pixels.

Step 3: A private key is used to determine the positions of embedding the watermark.

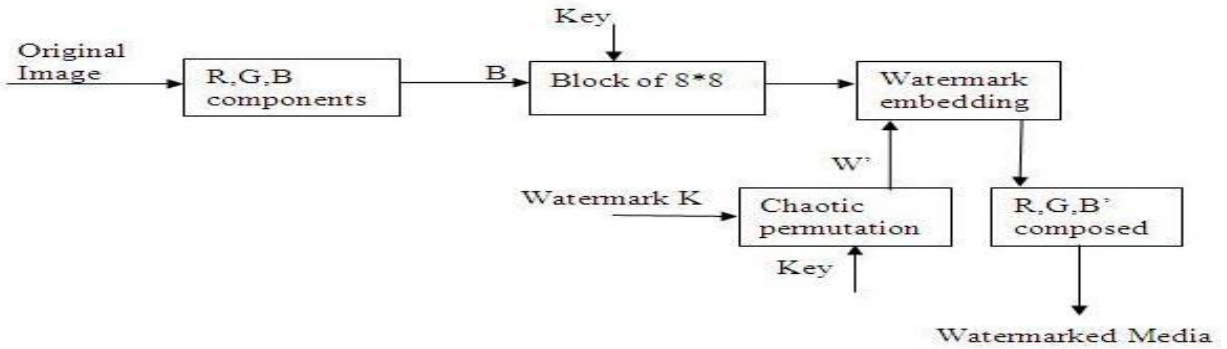

Fig.1.1: The proposed watermark-embedding scheme

Step 4: The encoded watermark W" is embedded in the blue component B. For each encoded watermark bit, a block of 8*8 is modified as follows:

If W"=1;

For all the pixels of the 8*8 blocks

{I'=I+ λ}

If W"=0;

For all the pixels of the 8*8 blocks

{I'=I- λ}

Where I' is the modified pixel intensity and I is the original intensity and λ is a constant.

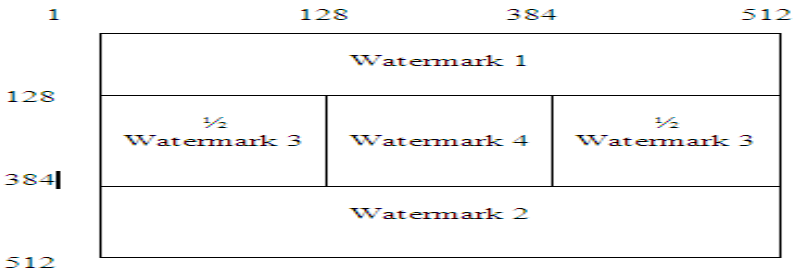

Fig.1.1.2: The proposed watermarks embedded positions

Step 5: The modified block of pixels is then positioned in its original location of the host image and then step 3 and 4 is repeated until all encoded watermark bits W" are embedded.
Step 6: After embedding the all encoded watermark bits four times, the R, G, and B' components are composed to obtain the watermarked image.

1.1.2 Watermark extraction

The proposed watermark extraction is shown in Fig. 1.1.3. It is required the original host image and the original watermark, therefore, it is a non-blind watermarking scheme. The proposed extraction is based on the probability (P1, P0) of detecting '1' or '0' bit, which can be obtained by comparing each pixel (I') in a block of 8*8 of the watermarked image with the corresponding pixel (I) in the original image and then the probability of detecting '1' or '0' bit is calculated as follows:

P1=P1+1/64 if I' > I
P0=P0+1/64 if I' ≤ I

According to the probability (P1, P0), the extracted watermark bits W" can be decoded as follows:

$W'' = 1$ if P1 ≥ P0
$W'' = 0$ if P1< P0

The extracted watermark bits for the four watermarks are decoded using Gray code and then, the decoded bits are XOR with random bits, which generated using the same secret key that was used during the watermark embedding. The decoded watermarks bits are reordering to images W'1, W'2, W'3, W'4. Together with the extraction of visual image watermark, we calculate the normalized cross correlation between the original watermark image W and the extracted watermarks W'1, W'2, W'3, W'4 to make a binary decision on whether a given watermark exists or not. We choose 0.5 as the threshold for watermark decision. The normalized cross correlation is defined by

$$NCC = \frac{\sum_i \sum_j W_{ij} W'_{ij}}{\sum_i \sum_j W_{ij}^2}$$

Where, Wij and W'ij are the pixel values at the position (i, j) of the original and the extracted watermark by that $1 \leq (i, j) \leq 32$, respectively.

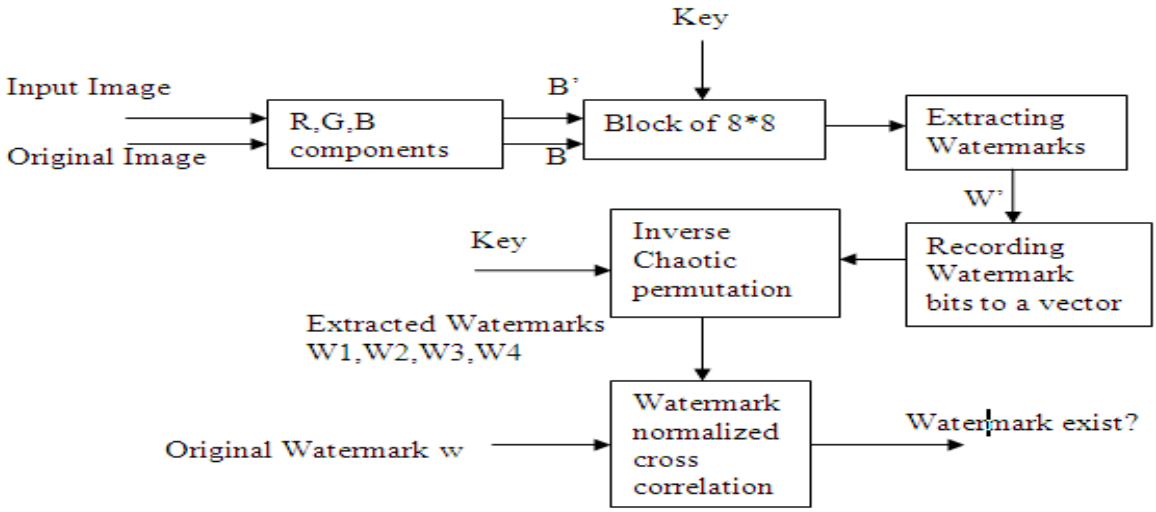

Fig. 1.1.3: The proposed watermark extraction scheme.

1.2 Video Watermarking

1.2.1 Video Embedding

This watermarking scheme embeds the watermark into the luminance values of the pixels, thus first does a conversion of the RGB (Red Green Blue) color space into the YCbCr (Luminance-Chrominance) color space is done:

$Y = 0.257R+0.576G+0.098B+16$

$C_b=-0.148R-0.291G+0.439B+128$ (1)

$C_r=0.439R+0.368G-0.071B+128$

After embedding, the video is converted back to the RGB format using Equation (2)

$R=1.164(Y-16)+1.596(C_r-128)$

$G=1.164(Y-16)-0.813(C_r-128)-0.391(C_b-128$ (2)

$B=1.164(Y-16)+2.018(C_b-128)$

To improve the resilience of the algorithm against different attacks we use three protection mechanics: error correction codes, redundant spatial embedding of one watermark bit into every block of $l \times l$ luminance pixels and redundant temporal embedding of the same watermark in every group of k frames. The inserted watermark is a binary image of resolution $h \times v$ depending on the size of the original video, the number of redundant frames and the error correction code used.

The algorithm uses a secret key K of 80 bits, 16 for the size of the watermark and 64 bits as seed for the pseudo-random number generator used to produce the code sequence *S*. The pseudo-random binary sequence S is used to spread the power spectrum of the watermark data, thus, increasing its robustness against attacks.

The watermark embedding process, illustrated in Fig.1.2.1 is described in the following steps:

a) The original video is partitioned into groups of *k* frames.

b) Every frame of the group is converted to the YCbCr format as in Equation 1.

c) The binary image matrix is transformed into a binary row vector *w* of size

$P=h \times v$ (3)

d) To protect the watermark against bit errors, a cyclic error correction code (*m*,*n*) with code word length of *m* bits and data word length of *n* bits is applied to the vector *w*. The size of the resulting watermark vector *wc* is:

$$P' = P\ (m/n) \qquad (4)$$

e) The binary sequence *wc* is partitioned into a number of $\frac{c}{k}$ sequences Wc (j) of size $p'\frac{k}{c}$ where $j=1$, $\frac{c}{k}$. The dimensions *h* and *v* of the watermark are chosen so that $p'\frac{k}{c}$ is an integer. The same sequence Wc(j) will be inserted into every frame of a group *j* of *k* frames.

f) The size *l* of a square block of $l \times l$ luminance values is calculated to embed a bit of the watermark:

$$l = \left[\sqrt{\frac{mnc}{p'k}}\right]$$

Where [.] is the integer part operator.

g) A spread-spectrum technique is used to spread the power spectrum of the watermark data, thus, increasing its robustness against attacks. First a binary pseudo-random code sequence of size

$$S = \{s_r | s_r \in \{0,1\}, r = 0,1,\ldots,l^2\}$$

l^2 with equal number of zeros and ones is generated using the Mersenne-Twister algorithm by Nishimura and Matsumoto with the use of the last 64 bits of the secret key *K* as seed for the generator. This method generates numbers with a period of $(2^{19937}-1)/2$.

h) For every bit of the watermark Wc(j) , the corresponding spread spectrum sequence is:

$$W_{ss} = \begin{cases} [s_1, s_2, \ldots s_{l^2}], \text{if } Wc = 0 \\ [\bar{s}_1, \bar{s}_2, \ldots, \bar{s}_{l^2}], \text{if } Wc = 1 \end{cases} \qquad (5)$$

i) A sequence *S* (representing one bit of the original watermark) is embedded in every block of $l \times l$ luminance values.

j) A bit of *S* is embedded into the luminance value of the pixel of the same index by rounding its value to an even or odd quantization level. Rounding to an even quantization level embeds a "0", while rounding to an odd quantization level embeds a "1", as shown in below Equation:

$$L_w(i,j) = \left|\frac{L(i,j)}{2q}\right| .2q + q, w, sign\left(L(i,j) - \left|\frac{L(i,j)}{2q}\right| .2q\right) \qquad (6)$$

Where $L(i, j)$ is the original luminance value, $L_w(i,j)$ is the watermarked luminance value of the pixel at position (i,j), *q* is the quantization step size and *sign*() is defined as:

$$\text{Sign}(x) = \begin{cases} -1, \text{if } x \leq 0 \\ 1, \text{if } x > 0 \end{cases} \qquad (7)$$

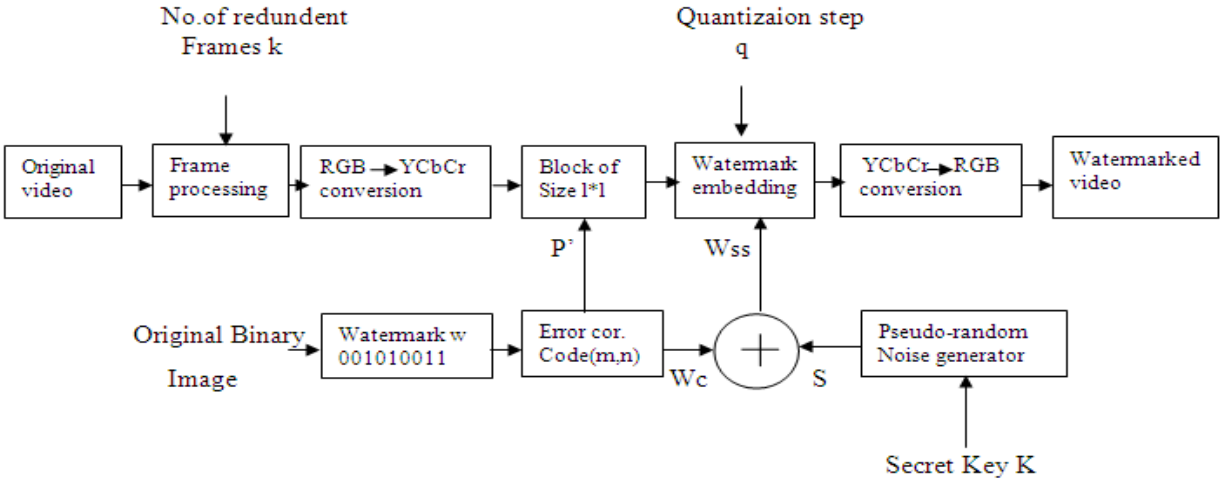

Fig. 1.2.1: Block diagram of the proposed watermark encoder

k) The video is converted back to the RGB format using Equation 2, obtaining the watermark video.

The choice of the quantization step q is a tradeoff between the perceptual quality of the watermarked video (q must have a small value) and the resilience of the watermarking scheme to attacks (q must have a big value). An example of embedding a watermark bit into a block of 4x4 pixels is given in Table 1.

Table 1: Embedding a watermark bit into a block of 4x4 luminance pixels

Wat. bit	Pseudorandom sequence S	Spread spectrum watermark $W_{ss} = S \square w$	Quant. Step	Original luminance Block	Watermarked luminance block
$W=0$	$\begin{bmatrix}0&1&1\\1&0&1\\0&1&0\\1&1&0\end{bmatrix}$	$\begin{bmatrix}0&1&1&0\\1&0&1&0\\0&1&0&1\\1&1&0&0\end{bmatrix}$	$q=4$	$\begin{bmatrix}224&75&86\\62&45&12\\45&5&68\\145&59&247\end{bmatrix}$	$\begin{bmatrix}224&76&84&24\\60&48&12&120\\48&4&72&76\\148&60&248&24\end{bmatrix}$
$W=1$		$\begin{bmatrix}1&0&0&1\\0&1&0&1\\1&0&1&0\\0&0&1&1\end{bmatrix}$			$\begin{bmatrix}228&72&88&20\\64&44&16&124\\48&8&68&72\\144&56&244&20\end{bmatrix}$

1.2.2 Video Extraction

The watermark extraction process, implies the following steps:

1. The watermarked video is partitioned into groups of k frames.
2. Every frame of the group is converted to the YCbCr format using Equation 1.
3. Every luminance frame is partitioned into square blocks of $l \times l$ luminance values.
4. A bit of the spread spectrum sequence W_{ss}' of size l^2 is extracted from every luminance value of a block of size $l \times l$ using Equation 8:

$$W' = mod\ 2\left(round\left(\frac{L_w(i,j)}{q}\right)\right) \qquad (8)$$

Where w' is the extracted watermark bit and mod 2(x) is the modulo2 function.

5. Using the 64 bit seed from the secret key K the binary sequence S is generated locally.
6. The extracted watermark bit of the corresponding block is:

$$Wb' = \begin{cases} 0, if \sum_{r=1}^{l^2} |W_{ss,r}' - S_r| \le \frac{l^2}{2} \\ 1, if \sum_{r=1}^{l^2} |W_{ss,r}' - S_r| > \frac{l^2}{2} \end{cases}$$

7. A binary sequence Wc,i'(j) is extracted from every frame of a group of k frames, where $i = \overline{1,k}$. The sequence Wc(j) is computed from Wc,i'(j) using Equation

$$Wc'(j) = \begin{cases} 0, dacă \sum_{i=1}^{k} W_{c,i}'(j) \le \frac{k}{2} \\ 1, dacă \sum_{i=1}^{k} W_{c,i}'(j) > \frac{k}{2} \end{cases},$$

$j \in \{1,2,3,\ldots,p'\}$

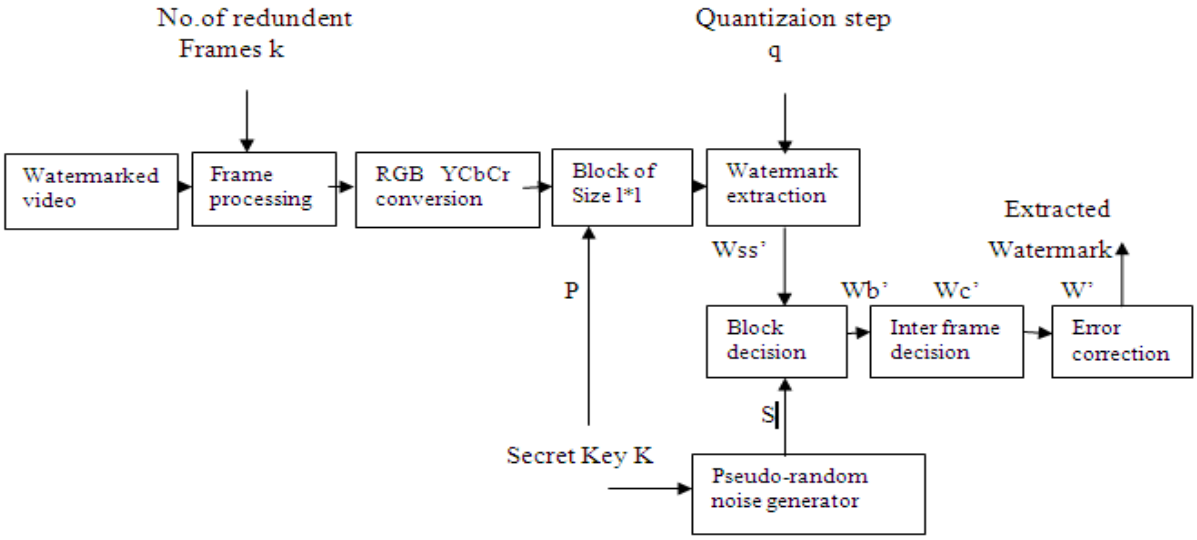

Fig.1.2.

2: Block diagram of the proposed watermark decoder

8. The resulting watermark bit stream Wc' of size *P'* is error corrected and the watermark *w* of size *P* is obtained.
9. The extracted binary image is obtained by reshaping the vector *w*′ to a matrix of size $h \times v$.

CONCLUSIONS

A robust watermark scheme based on a block probability for color image is presented, which operates in spatial domain by embedding the watermark image four times in different positions in order to be robust for cropping attack. The extraction of the watermark depends on the original image, so it is a non-blind watermarking scheme.

This is a novel video watermarking technique based on the quantization of the luminance values of pixel blocks. The algorithm uses error correction codes to protect the inserted watermark and temporal redundancy to embed the same watermark in different frames of the video. The watermarks used were binary images containing the name of the author. The advantage of using binary images instead of pseudo-random noise is that even a watermark extracted with a high decoding BER can be visually identified. The proposed technique also achieves good resilience against different attacks in the spatial domain.

REFERENCES

1. A new robust watermarking scheme for color image in spatial domain Ibrahim nasir, ying weng, jianmin jiang school of informatics, university of bradford,uk{ianasir,y.weng,j.jiang}@brandford.ac.uk
2. New robust watermarking scheme for video copyright protection in the spatial domain - radu ovidiu preda1, nicolae vizireanu2 u.p.b. sci. bull., series c, vol. 73, iss. 1, 2011 issn 1454-234x
3. http://en.wikipedia.org/wiki/digitalwatermarking
4. https://www.cl.cam.ac.uk/teaching/0910/r08/work/essay-ma485-watermarking.pdf
5. http://informatika.stei.itb.ac.id/~rinaldi.munir/kriptografi/wmsurvey1999mohanty.pdf

