Watermarking Method with Exact Self-Propagating Restoration Capabilities

S. Bravo-Solorio ◇[1], C.-T. Li ◇[2], A. K. Nandi ⋆[3]

◇ *Computer Science Department, The University of Warwick*
Coventry, CV4 7AL, UK
[1] s.bravo-solorio@warwick.ac.uk
[2] c-t.li@warwick.ac.uk

⋆ *Electrical Engineering and Electronics Department, The University of Liverpool*
Brownlow Hill, Liverpool, L69 3GJ, UK
[3] a.nandi@liverpool.ac.uk

***Abstract*—This paper proposes a new fragile watermarking capable of perfectly restoring the original watermarked pixels of a tampered image. First, a secure block-wise mechanism, resilient to cropping, is used to localise tampered blocks of pixels. The authentic pixels and some reference bits are then used to estimate the original 5 most significant bits (MSBs) of the tampered pixels by means of an exhaustive and iterative restoration mechanism. Results are presented to demonstrate the restoration capabilities of the proposed mechanism.**

I. Introduction

Fragile watermarking describe techniques to insert information imperceptibly (i.e. a *watermark*) in digital images, so that distortions in the content can be indirectly exposed by changes in its watermark [1], [2]. Furthermore, the fact that the watermark undergoes the same distortions as the cover images opens up the possibility of not only detecting tampered regions, but also restoring the altered contents to its original state, before the manipulation took place.

The restoration mechanism can be either *approximate* or *exact*. Schemes with approximate restoration capabilities can recover a coarse version of the original content, even if the tampered region is considerably large [3]–[8]. Nonetheless, the quality of the restored content may be insufficient for some applications.

Schemes with exact restoration capabilities can perfectly reconstruct the original content, provided that the altered region is not too large. In [9], some reference bits generated from the 5 most significant bit-planes (MSBPs) of the image are inserted using a reversible embedding mechanism. At the receiver end, a portion of the watermark is employed to localise tampered pixel-blocks, while the reference bits allocated in authentic pixels are used to reconstruct the original content perfectly. Nevertheless, this can be achieved only if the tampered area covers less than 3.2% of the image. Zhang and Wang [10] proposed a method, whereby the 5 MSBs of every altered pixel can be accurately estimated by means of exhaustive attempts, as long as the portion of tampered pixels is less than 6.6% of the image. In [11], tampered pixel-blocks are localised by means of a block-wise method resilient to cropping, while an exhaustive mechanism uses the watermark derived from the 5 MSBPs of the image to enhance the tampering localisation and restore the exact content. However, only a portion of the pixels can be restored with this mechanism. Zhang *et al.* [12] proposed a scheme, whereby some reference bits calculated with the 5 MSBs of pairs of pixels are used to reconstruct the original content of altered regions. When the exact content could not be restored, an approximation is estimated exhaustively. The same authors proposed an elegant restoration mechanism in [7]. Here, a system of linear equations is formed with a vector of reference bits allocated in authentic pixels, the bits of the authentic pixels and a binary pseudo-random matrix. Then, the system is solved to calculate the original bits of the altered pixels. The scheme manages to restore the original content of an altered region that covers up to 24%–28% of the image, depending on the settings of the algorithm and the image size.

In this paper, a secure block-wise method is used to localise altered blocks of pixels, even when the watermarked image has been cropped. Additionally, some reference bits are used to identify a set of *potential restoration candidates* for each tampered pixel, considering the authentic surrounding pixels. The sets are subsequently refined to find to the correct 5 MSBs of each tampered pixel. The rest of the paper is structured as follows. Section II describes the proposed method and some results are reported in Section III. Finally, some conclusions are given in Section IV.

II. Proposed Method

Consider an 8-bit grey-scale image sized $n_1 \times n_2$. Assuming that both n_1 and n_2 are multiples of 8, denote the total number of pixels as $n(= n_1 n_2)$. A pixel can be represented by 8 bits denoted as $b_1, b_2, \ldots, b_8$, where b_1 is the least significant bit (LSB) and b_8 is the MSB.

A. Embedding Process

Using a secret key k_1, the image is pseudo-randomly divided into subsets of m pixels each, thereby generating a total of

WIFS‘2012, December, 2-5, 2012, Tenerife, Spain. 978-1-4244-9080-6/10/$26.00 ©2012 IEEE.

n_{s} $(= n/m)$ subsets. Let $x_{i,1},\dots,x_{i,m}$ denote the pixels in the i-th subset. An m-bit code is computed using the bits, $b_4,\dots,b_7$, of every pixel in the subset; that is,

$$r_i = \mathcal{H}(\hat{x}_{i,1},\dots,\hat{x}_{i,m}) \ , \qquad (1)$$

where $\mathcal{H}(\cdot)$ is a cryptographic hash function (e.g. SHA algorithm [13]) and, $\hat{x}_{i,j} \in [0,15]$ is given by,

$$\hat{x}_{i,j} = \lfloor x_{i,j}/8 \rfloor \mod 16 \ , j = 1,\dots,m. \qquad (2)$$

Observe that the value of $\hat{x}_{i,j}$ is given by the bits $b_4,\dots,b_7$ of $x_{i,j}$. The most significant bit b_8 is not considered in (2) to constrain the search of potential restoration candidates and enable the filtering mechanism detailed in Section II-C.

The code r_i can be represented as the sequence of bits $r_{i,1},\dots,r_{i,m}$, called *reference bits*, which are subsequently embedded in the bit b_3 of every pixel in the subset as,

$$x^w_{i,j} = (\lfloor x_{i,j}/8 \rfloor \times 8) + (r_{i,j} \times 4) \ , j = 1,\dots,m \ . \qquad (3)$$

A second set of reference bits are generated by dividing the image into subsets of m pixels each, but now using second secret key k_2. The idea behind the two different keys is to associate every pixel to two different subsets. So, in practise, k_2 can be defined as a function of k_1, without compromising the security of the scheme. An m-bit code is computed using the 5 MSBs of every pixel in every i-th subset as,

$$r_i = \mathcal{H}(\check{x}_{i,1},\dots,\check{x}_{i,m}) \ , \qquad (4)$$

where $\check{x}_{i,j} \in [0,31]$ is given by,

$$\check{x}_{i,j} = \lfloor x_{i,j}/8 \rfloor \ , j = 1,\dots,m \ . \qquad (5)$$

The resulting reference bits $r_{i,1},\dots,r_{i,m}$ are embedded in the bit b_2 of every pixel in the subset as,

$$x^w_{i,j} = x^w_{i,j} + (r_{i,j} \times 2) \ , j = 1,\dots,m \ . \qquad (6)$$

Because the security of the restoration mechanism relies on the immense number of possible combinations of pixel subsets, we have assumed that to use keyed hashes in (1) and (4) is unnecessary.

To enable the detection and localisation of tampered pixel-blocks, we adopted the secure block-wise method resilient to cropping in [11], which is a tailored version of the method in [14]. Divide the watermarked image into non-overlapping blocks of 8×8 pixels, and denote the total number of blocks as n_{b} $(= n/64)$. For each block, a 64-bit description code is encoded as, $\mathcal{I} \,||\, n_1 \,||\, n_2 \,||\, p$, where $\mathcal{I}$ is an image index exclusively associated to the image, p denotes the block index (of the p-th block), and $||$ denotes concatenation of bits. Note that all the description bits share a *common prefix* (i.e. $\mathcal{I} \,||\, n_1 \,||\, n_2$); let Λ denote the length of the common prefix. This information can be decoded by the detector to localise possible tampered pixel-blocks and, in case of cropping, restore the original shape of the image, while correcting any possible displacement of the content. Additionally, a 64-bit has code is generated by means of a cryptographic hash function fed with the the 7 MSBPs of the block (i.e. the bits $b_2,\dots,b_8$ of every pixel in the block). The exclusive-or operation between the description code and the hash code is computed to generate a 64-bit authentication code,

$$a_{p,j} = w_{p,j} \oplus h_{p,j} \ ; \, p = 1,\dots,n_{\mathrm{b}}, \text{ and, } j = 1,\dots,64 \ , \qquad (7)$$

where $w_{p,j}$ is the j-th bit of the hash code of the p-th block, $h_{p,j}$ is the j-th bit of the description code of the p-th block, and $a_{p,j}$ is the j-th bit of the authentication code of the p-th block. The least significant bit-plane (LSBP) of the p-th block is replaced with the encrypted version of the authentication code of the same bit-length.

To estimate the average distortion inflicted to host images, let us assume that the distribution of the embedded watermarks is uniform. This is a reasonable assumption, because of the characteristics of cryptographic hash codes. Since the 3 LSBPs of the image are being replaced by the watermarks, the average energy of the distortion on each pixel is,

$$E = \frac{1}{64} \sum_{i=0}^{3} \sum_{j=0}^{3} (i-j)^2 = \frac{21}{2} \ , \qquad (8)$$

so, the average peak signal-to-noise ratio (PSNR) is,

$$\text{PSNR} \approx 10 \log_{10} \left(\frac{2 \times 255^2}{21} \right) = 37.9 \text{ dB} \qquad (9)$$

B. Tampering Localisation and Cropping Survival

Divide the input image, sized $n'_1 \times n'_2$, into non-overlapping blocks of 8×8 pixels and denote the total number of blocks as n'_{b}. The 64-bit sequence retrieved from the LSBP of each block is decrypted to obtain its corresponding 64-bit authentication code. Additionally, a 64-bit hash code is generated with a cryptographic hash function fed with the 7 MSBPs of each block. The bits of the description code of every block are decoded by,

$$w'_{p,j} = a'_{p,j} \oplus h'_{p,j}; \, p = 1,\dots,n'_{\mathrm{b}}, \text{ and, } j = 1,\dots,64 \ , \qquad (10)$$

where $a'_{p,j}$ is the j-th bit of the authentication code of the p-th block, $h'_{p,j}$ is the j-th bit of the hash code of the p-th block, and $a'_{p,j}$ is the j-th bit of the description code of the p-th block. Let $\mathbf{A}$ be a set of description codes, whose Λ MSBs are identical to each other. If the image has been watermarked, the number of elements in the set $\mathbf{A}$ – i.e. the cardinality $|\mathbf{A}|$ – is expected to be higher than a threshold τ_L.

If $|\mathbf{A}| \leq \tau_L$, 64 shifted versions of the image are analysed as above. In every shifted version, all the pixels in the image are displaced λ_i rows and λ_j columns, for $i = 0, -1, \dots, -8$ and $j = 0, -1, \dots, -8$. This enables the authentication of images whose left/upper-most edges have been removed by cropping. If none of the shifted versions was regarded as watermarked, the detection process is terminated altogether. The probability that a non-watermarked image will be misjudged as watermarked can be modelled by,

$$\mathcal{P}_{D1} = \left[1 - \sum_{q=0}^{\tau_L} \binom{n'_{\mathrm{b}}}{q} 2^{-q\Lambda}(1-2^{-\Lambda})^{n'_{\mathrm{b}}-q}\right] \times 64 \ , \quad (11)$$

where $\binom{n'_{\mathrm{b}}}{q}$ is the binomial coefficient.

If the image is regarded as watermarked, retrieve n_1 and n_2 from the common prefix of the description codes with higher occurrence, and restore the original shape of the image in case of cropping. Additionally, the block index retrieved from the description codes are used to estimate a possible *common displacement* to translate the authentic content to its original location, thereby resynchronising the watermark with the restoration mechanism detailed below. The blocks associated to the tampered bit strings are then localised in a bitmap.

C. Self-Propagating Restoration

Once the tampered blocks have been properly localised, the following mechanism is executed to estimate the original 5 MSBs of the tampered pixels. The pixels and the reference bits allocated in unaltered pixel-blocks will be referred to as *reserved pixels* and *reserved reference bits*, respectively.

Step 1: Here, the goal is to find a set of *potential restoration candidates* for every tampered pixel in a subset. The following procedure is only executed for subsets containing at least one tampered pixel.

Using the key k_1, the image is pseudo-randomly divided into subsets of m pixels each to generate a total of n_{s} subsets. Let $y_{i,1}, \ldots, y_{i,m}$ be the pixels of the i-th subset, for $i = 1, \ldots, n_{\mathrm{s}}$, and c_i be the number of tampered pixels in the subset. The remainder of this step is executed for every i-th subset, provided that $c_i \leq 3$. Tampered pixels in subsets with more than 3 altered pixels will be associated to a set of potential restoration candidates containing all the possible 5-bit values $0, \ldots, 31$, and the remainder of the step will be skipped. The probability that the condition above will be met for a subset is given by,

$$\mathcal{P}_{R1} = \sum_{q=1}^{3} \binom{m}{q} \alpha^q (1-\alpha)^{m-q} \ , \quad (12)$$

where α is the is the ratio between the number of tampered pixels and the total number of pixels.

Let $r'_{i,1}, \ldots, r'_{i,m}$ be the reference bits retrieved from the bit b_3 of every pixel in the i-th subset,

$$r'_{i,j} = \lfloor y_{i,j}/4 \rfloor \mod 2, \; j = 1, \ldots, m \ . \quad (13)$$

Some m-bit test codes are computed as, $\mathcal{H}(\hat{y}_{i,1}, \ldots, \hat{y}_{i,m})$, where $\hat{y}_{i,j} = (\lfloor y_{i,j}/8 \rfloor \mod 16)$ if $y_{i,j}$ is a reserved pixel, otherwise, it exhaustively takes all the 4-bit values $\hat{y}_{i,j} = 0, \ldots, 15$. A total of $n_{\mathrm{c}} (= 16^{c_i})$ test codes will be generated and compared with the retrieved reference bits (and considering only its reserved bits) to identify the 4-bit values that led to a match. Let $\beta (= 2^{c_i - m})$ denote the probability that a test code will produce a match. The probability that the number of test codes that will lead to a match equals any given t can be estimated as,

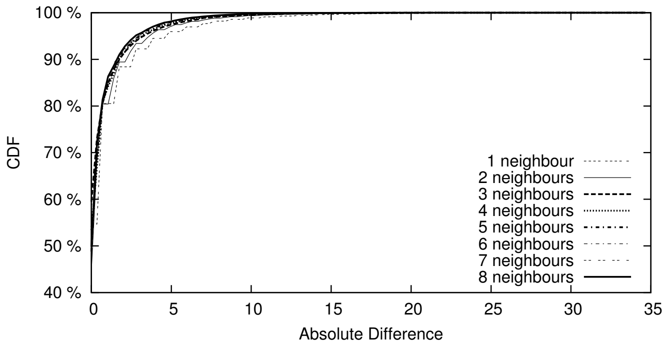


Fig. 1: In nearly 94% of the pixels, in a data set with over 1000 natural images, the absolute difference between the 5 MSBs of a pixel and the mean estimated from the 5 MSBs of its neighbours was below 5.

$$\mathcal{P}_{R2} = \binom{n_{\mathrm{c}}}{t} \beta^t (1-\beta)^{n_{\mathrm{c}}-t} \ , \quad (14)$$

The 4-bit values that led to a match are subsequently extended to form a set of 5-bit potential restoration candidates associated to every tampered pixel. For example, consider that a matching test code obtained as the combination of two tampered pixels, say $\hat{y}_{i,u} = 4$ and $\hat{y}_{i,v} = 13$, whose binary representation will become the 4 MSBs of a pair of extended 5-bit values. That is, $4_{10} = 0100_2$ will be extended to the pair $4_{10} = 00100_2$ and $20_{10} = 10100_2$, while $13_{10} = 1101_2$ will be extended to the pair $13_{10} = 01101_2$ and $29_{10} = 11101_2$. Thus, the sets of potential restoration candidates $\mathbf{R}_u = \{4, 20\}$ and $\mathbf{R}_v = \{13, 29\}$ will be associated to the pixels $y_{i,u}$ $y_{i,v}$, respectively. However, an extended value is discarded from the set if the other extended value in the pair is sufficiently close to the average estimated with the 5 MSBs of the reserved pixels surrounding the tampered pixel. For example, let μ_u be the mean calculated with the 5 MSBs of the reserved pixels around $y_{i,u}$. If $|\mu_u - 4| < \tau_\mu$, where τ_μ is a predefined threshold, the value 20 is discarded, resulting in a refined set $\mathbf{R}_u = \{4\}$. This filtering rule stemmed from empirical observations made on a data set containing over 1000 natural images. We noticed that, in over 94% of the cases, the absolute difference between the 5 MSBs of a pixel and the mean estimated with the 5 MSBs of a subset of its neighbouring pixels is less than 5 (in fact, in our experiments, we set $\tau_\mu = 5$). The comparison between the pixels in the data set and the a mean calculated using a subset of 1 to 8 neighbours is shown in Fig. 1.

Step 2: The aim of this step is to refine the set of potential restoration candidates associated to each altered pixel in an attempt to find a unique restoration candidate.

Once again, the image is divided into subsets of m pixels each, but now using the key k_2. Denote as $r'_{i,1}, \ldots, r'_{i,m}$ the

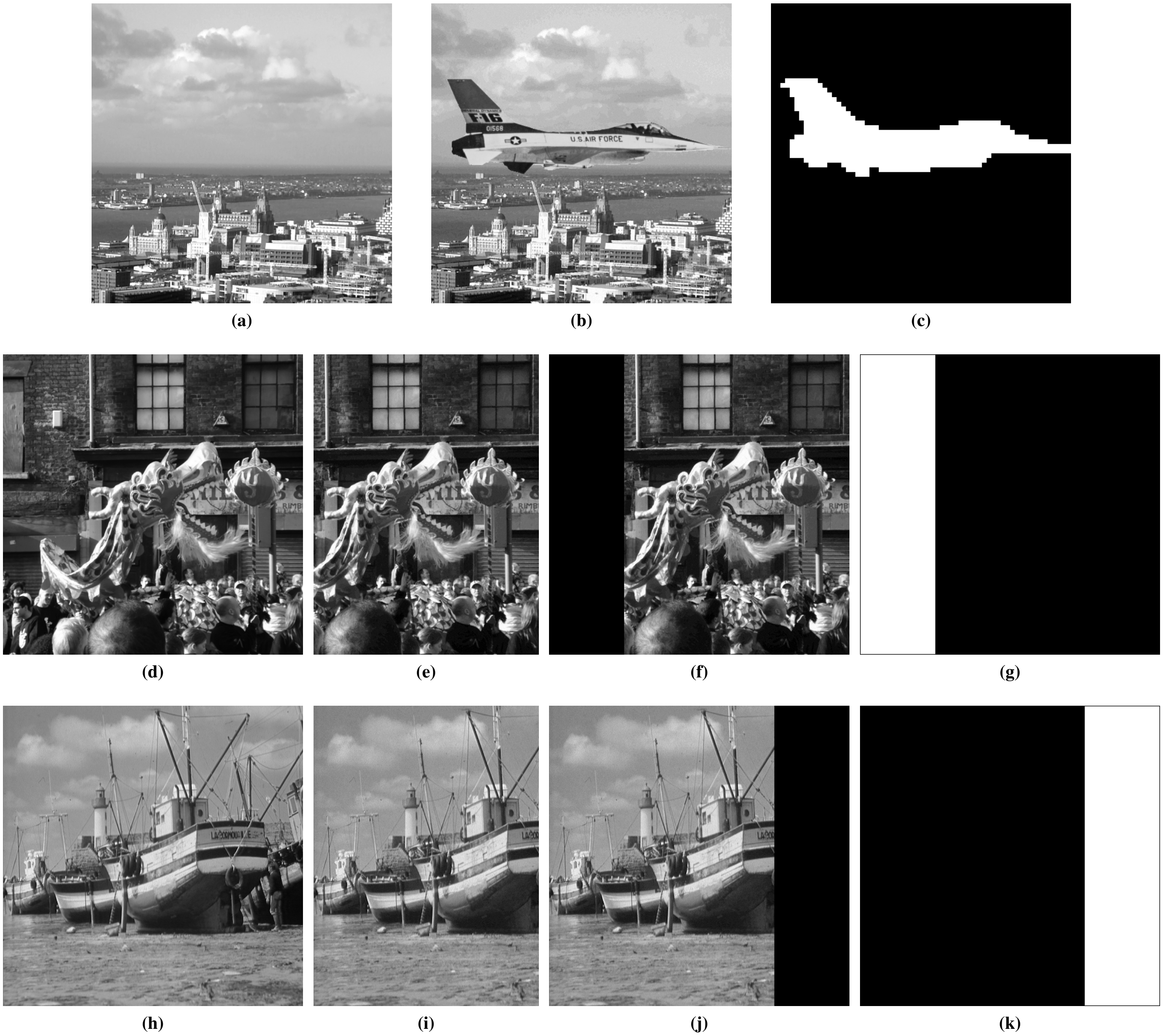


Fig. 2: Experiments on three images: (a) Waterfront, (d) Dragon and (h) Boat. (b) Tampered version of (a). (c) Tampered region localised in (b). (e) Cropped version of (d). (f) Corrected image-shape and displacement from (e). (g) Tampered region localised in (f). (i) Cropped version of (h). (j) Corrected image shape and displacement from (i). (k) Tampered region localised in (j).

reference bits extracted from the bit b_2 of every pixel in the i-th subset,

$$r'_{i,j} = \lfloor y_{i,j}/2 \rfloor \mod 2,\, j = 1, \dots, m \ . \tag{15}$$

Some m-bit test codes are computed as, $\mathcal{H}(\breve{y}_{i,1}, \dots, \breve{y}_{i,m})$, where $\breve{y}_{i,j} = \lfloor y_{i,j}/8 \rfloor$ if $y_{i,j}$ is a reserved pixel, otherwise, it exhaustively takes all the potential values in its associated set $\mathbf{R}_j$. Every text code is compared with the retrieved reference code, considering only the reserved bits. The elements in $\mathbf{R}_j$ that did not lead to a mach are discarded from the set. Finally, the 5 MSBs of the altered pixels associated to a single potential restoration candidate can be readely recovered.

Iterations: Step 1 and Step 2 are iteratively repeated until no further pixels can be restored.

Although a comprehensive probabilistic analysis of the proposed restoration mechanism is on its way, there is an interesting property that can provide valuable hints about the effectiveness of the proposed restoration mechanism. In particular, observe that the ratio α decreases as the number of restored pixels grows after each iteration, thereby increasing the probability $\mathcal{P}_{R1}$ and reducing the probability $\mathcal{P}_{R2}$ for

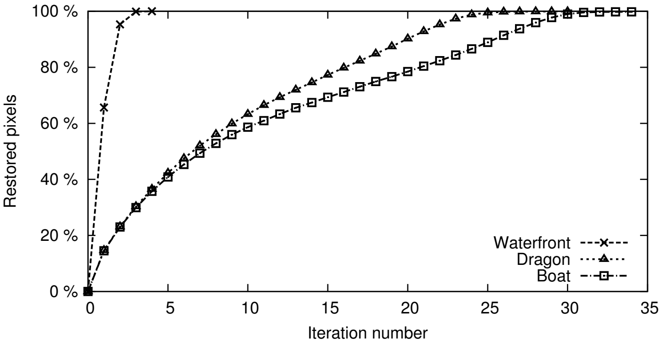


Fig. 4: Cumulative percentage of pixels restored in different iterations.

larger values of t. In other words, the chances that a tampered pixel can be restored in future iterations increases as the number of restored pixels grows, resulting in an apparent *self-propagating* effect in the restoration mechanism. However, it fails when the initial ratio of tampered pixels is too large (typically above 25% of the image).

III. Results

The used 512×512 test images are shown in Figs. 2(a) (Waterfront image), 2(d) (Dragon image) and 2(h) (Boat image). The following settings were empirically found to deliver the best performance: $\tau_L = 20$ (less than 0.05% of the total number of pixel-blocks), $m = 16$ and $\tau_\mu = 5$. The average PSNR between the original test images and their watermarked version was assessed to be 37.87 dB, which is consistent with the predicted embedding distortion in Eq. (9).

First, a doctored image was generated by placing a jet fighter at the centre of the watermarked version of the Waterfront image, as shown in Fig. 2(b). The pixel-blocs regarded as altered are depicted as a white region in Fig. 2(c). As illustrated in Fig. 4, the cumulative percentage of restored pixels increased sharply from 65% in the first iteration, to 100% in the iteration 4.

To demonstrate the resilience capabilities of the proposed method against cropping, 25% of the pixels in the watermarked versions of the Dragon and the Boat images were cut off to generate the 512×384 images in Figs. 2(e) and 2(i). The cropped portions were the left-most columns in the Dragon image and the right-most columns in the Boat image. The system managed to restore the original shape of the cropped images, while displacing the authentic pixel-blocks to its original location, as illustrated in Figs. 2(f) and 2(j). The missing pixels identified in the tampering localisation maps are shown in Figs. 2(g) and 2(k). As illustrated in Fig. 4, the restoration mechanism required 30 iterations to restore 99.92% of the missing pixels of the Dragon image and 34 iterations to restore 99.94% of the missing pixels of the boat image. Observe that the cumulative percentage of restored pixels gradually increased as the number of iterations grew. The sequence of images shown in Figs. 3(a) to 3(d) are the images resulting from iterations 5, 15, 25 and 30, respectively, of the execution of the restoration mechanism on the image in Fig. 2(j).

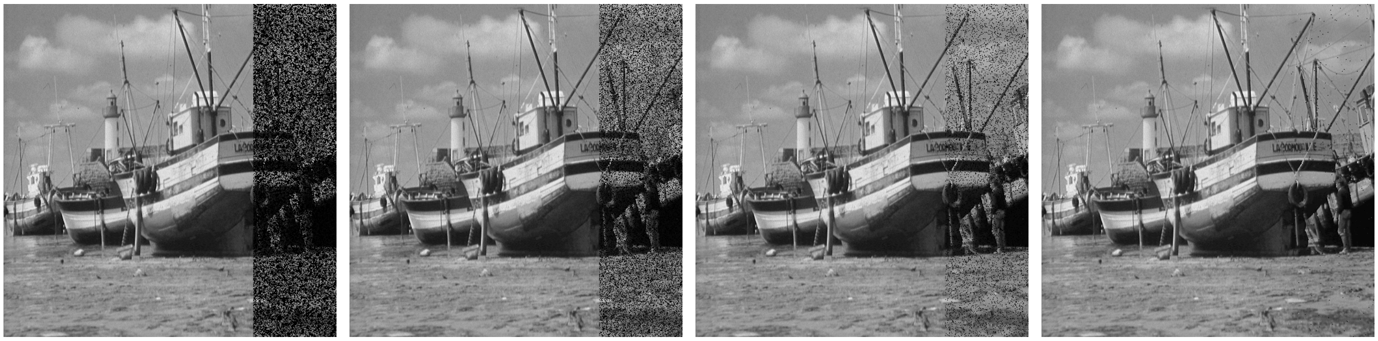
A comparison of various watermarking methods with restoration capabilities is presented in Table I. There is an evident trade-off between the maximum proportion of tampered pixels that can be restored and the quality of the recovered areas. The methods in [15] and [8] are the ones that cause the lesser embedding distortion. However, because of the *tampering coincidence problem*, detailed in [7], the method in [15] cannot recover all the pixels, even if the altered area covers only a small proportion of the pixels in the image (e.g. 20%). The schemes in [3], and [7] (method 2) provide approximate restoration capabilities of corrupted areas as large as 59% and 66% of the image, respectively. In these methods, the smaller the altered area, the higher the quality of the reconstructed content. The method in [5] provides high-quality restoration capabilities of images containing altered areas that cover up to 35% of the pixels. The latest three methods in the table afford exact restoration capabilities. Nonetheless, the method in [10] works only when the tampered region covers less than 6.6% of the image. On the other hand, the method in [7] (method 1) can restore images with tampered portions of up to 24%–28% of the image, depending on the initial settings and the image size. However, not even a single pixel can be recovered from cropped images. In contrast, the proposed method can reconstruct the original content of images that have been tampered or cropped up to 23%–25% of the image, depending on the texture properties of the image. Although extensive experiments on a large image data set are on their way, so far, we have observed that the proposed scheme achieves a better restoration performance when the altered region is predominantly low-textured. This is because the original value of a tampered pixel in a low-textured area can be more easily predicted by its authentic neighbours in the filtering mechanism of potential restoration candidates.

IV. Conclusions

A new watermarking mechanism with exact restoration capabilities has been presented. The scheme relies on a secure mechanism, resilient to cropping, which localises blocks of altered pixels. Additionally, some reference bits and the surviving authentic pixels are exhaustively examined to identify a set potential restoration candidates of each tampered pixel, which is subsequently refined to estimate its original 5 MSBs. The procedure is iteratively repeated until no further pixels can be recovered. Results show that the proposed scheme manages to reconstruct the original content when the altered or cropped area represents up to 25% of the total number of pixels in the image.

Acknowledgement

This paper is supported by the National Council of Science and Technology (CONACyT) Mexico, UK Technology Strategy Board project 4347-35177 and EU FP7 DIVEFOR project (Grant Agreement No. 251677)



(a) Iteration 5 **(b)** Iteration 15 **(c)** Iteration 25 **(d)** Iteration 30

Fig. 3: Sequence of the restoration of the image in Fig. 2(j) in iteration 5, 15, 25 and 30.

TABLE I: Performance comparison.

Method	**Average embedding distortion (PSNR)**	**Average restoration quality (PNSR)**	**Cropping**	**Condition for restoration**
Method in [15]	44.2 dB	29.9 dB	No	Limited by the tampering coincidence problem
Method in [3]	37.9 dB	[26,29] dB	No	Tampered area $< 59\%$
Method in [5]	37.9 dB	35.0 dB	No	Tampered area $< 35\%$
Method 2 in [7]	37.9 dB	[22,40] dB	No	Tampered area $< 66\%$
Method in [8]	44.2 dB	29.9 dB	Yes	Tampered area $< 33\%$
Method in [10]	37.9 dB	$+\infty$	No	Tampered area $< 6.6\%$
Method 1 in [7]	37.9 dB	$+\infty$	No	Tampered area $< 24\%$ – 28%
Proposed method	37.9 dB	$+\infty$	Yes	Tampered area $< 23\%$ – 25%

References

[1] C.-T. Li and Y. Yuan, "Digital watermarking scheme exploiting nondeterministic dependence for image authentication," *Optical Engineering*, vol. 45, no. 12, pp. 127 001–1–6, 2006.

[2] Y. Yang, X. Sun, H. Yang, C.-T. Li, and R. Xiao, "A contrast-sensitive reversible visible image watermarking technique," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 5, pp. 656–667, 2009.

[3] X. Zhang, S. Wang, and G. Feng, "Fragile watermarking scheme with extensive content restoration capability," in *Proc. of IWDW – International Workshop on Digital Watermarking*, 2009, pp. 268–278.

[4] H. J. He, J. S. Zhang, and F. Chen, "A self-recovery fragile watermarking scheme for image authentication with superior localization," *Science in China Series F: Information Sciences*, vol. 51, no. 10, pp. 1487–1507, 2008.

[5] Z. Qian, G. Feng, X. Zhang, and S. Wang, "Image self-embedding with high-quality restoration capability," *Digital Signal Processing*, vol. 21, no. 2, pp. 278–286, 2011.

[6] X. Zhang, Z. Qian, Y. Ren, and G. Feng, "Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 4, pp. 1223–1232, 2011.

[7] X. Zhang, S. Wang, Z. Qian, and G. Feng, "Reference sharing mechanism for watermark self-embedding," *IEEE Transactions on Image Processing*, vol. 20, no. 2, pp. 485–495, 2011.

[8] S. Bravo-Solorio, C.-T. Li, and A. K. Nandi, "Watermarking with low embedding distortion and self-propagating restoration capabilities," in *Proc. of ICIP – IEEE International Conference on Image Processing*, 2012, (Accepted).

[9] X. Zhang and S. Wang, "Fragile watermarking with error-free restoration capability," *IEEE Transactions on Multimedia*, vol. 10, no. 8, pp. 1490–1499, 2008.

[10] ——, "Fragile watermarking scheme using a hierarchical mechanism," *Signal Processing*, vol. 89, no. 4, pp. 675–679, 2009.

[11] S. Bravo-Solorio and A. K. Nandi, "Secure fragile watermarking method for image authentication with improved tampering localisation and self-recovery capabilities," *Signal Processing*, vol. 91, no. 4, pp. 728–739, 2011.

[12] X. Zhang, S. Wang, Z. Qian, and G. Feng, "Self-embedding watermark with flexible restoration quality," *Multimedia Tools and Applications*, vol. 54, no. 2, pp. 385–395, 2010.

[13] *Secure Hash Standard*. Washington: National Institute of Standards and Technology, 2002, federal Information Processing Standard 180-182. [Online]. Available: http://csrc.nist.gov/publications/fips/

[14] J. Fridrich, "Security of fragile authentication watermarks with localization," in *Proc. of Security and Watermarking of Multimedia Contents*, vol. 4675. CA, USA: SPIE, 2002, pp. 691 – 700.

[15] P.-L. Lin, C.-K. Hsie, and P.-W. Huang, "A hierarchical digital watermarking method for image tamper detection and recovery," *Pattern Recognition*, vol. 38, no. 12, pp. 2519 – 2529, 2005.