Chapter 5

Authentication Watermarking with Tamper Detection and Recovery (AW-TDR)

5.1 Introduction

In this chapter, we present an efficient and effective watermarking method for image tamper detection and recovery. This chapter is structured as follows:

- Section 5.2 reviews authentication watermarking by Wong (1998) as a basis for discussion on vector quantization counterfeiting attacks.
- Section 5.3 describes vector quantization (VQ) counterfeiting attacks on block-wise independent watermarking schemes.
- Section 5.4 discusses a few techniques as countermeasures against VQ counterfeiting attacks. These include increasing block dimension, breaking block-wise independent and using a hierarchical watermarking technique.
- Section 5.5 proposes an authentication watermarking technique with tamper detection and recovery (AW-TDR).

5.2 Block-based Authentication Watermark

A block-based watermarking technique (Wong 1998) used an M x N image X and a binary watermark image W. In practice, this step is usually achieved by tiling the original image with a smaller logo image.

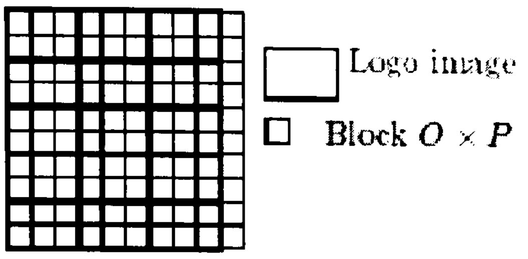


Figure 5. 1 Tiling of logo image in Wong's scheme

The original image X is partitioned into O x P pixel blocks, $\{X_1, X_2, \ldots\}$; where X_r denotes such blocks. Likewise, the watermark image is partitioned into blocks, W_r. For each block X_r, a corresponding block $\tilde{X}_r$ is formed by setting the least significant bit of each pixel to zero. A cryptographic hash (e.g.,. MD5 or SHA) of transformed block $\tilde{X}_r$ and image dimensions is computed.

$$H_r = \mathrm{H}(M, N, \tilde{X}_r) \tag{5.1}$$

The signature of a block is formed by XORing the computed hash with the watermark pattern and encrypting the result with a public key encryption algorithm.

$$S_r = Encrypt(H_r \oplus W_r, Key_{private}) \tag{5.2}$$

where $\oplus$ denotes the bitwise XOR operator. Finally, the signature S_r is inserted in X_r as the least significant bits of the block. Note that the application of this procedure independently on each block produces the watermarked image.

During watermark verification similar steps are followed. First the candidate image $\tilde{X}$ is partitioned into blocks $\tilde{X}_r$. Signature $\tilde{S}_r$ is read from the least significant bits of each block, $\widetilde{X}_r$. $\widetilde{X}_r$s are formed by setting LSBs to zero and $\widetilde{H}_r$s are calculated using image sizes and $\widetilde{X}_r$s. Finally, watermark image blocks are recovered by XORing the hash values with decrypted signatures from each block.

$$\widetilde{W}_r = Decrypt(\widetilde{S}_r, Keypublic) \oplus \widetilde{H}_r \qquad (5.3)$$

Any changes in the pixel values of a block alter either the decrypted signature or (with very high probability) the output of the hash function. Theoretically, a randomly generated block may carry the correct watermark pattern. Nevertheless, the probability of such an occurrence is practically negligible. In either case, the recovered watermark block $\widetilde{W}_r$ will be significantly different than the embedded watermark block. As a result, when a group of pixels in a spatial region are altered, the manipulation will be detected by the change in the corresponding region of the binary watermark image. On the other hand, it is possible to replace an entire image block with another without arousing suspicion, provided that both blocks bear the same watermark pattern. This observation is the basis for the vector quantization attack described in the next section.

5.3 Vector Quantization Counterfeiting Attack

A counterfeiting attack on block-wise independent watermarking schemes was proposed by Holliman and Memon (2000). The attacker approximates an image for which he wishes to create a forgery by using a collage of authentic blocks from watermarked images. Since the embedding and authentication processes are block-wise, the verification algorithm authenticates the collage image. Given a large enough database of watermarked images, the attacker can ensure that the counterfeit collage image has the same visual appearance as his original unwatermarked image.

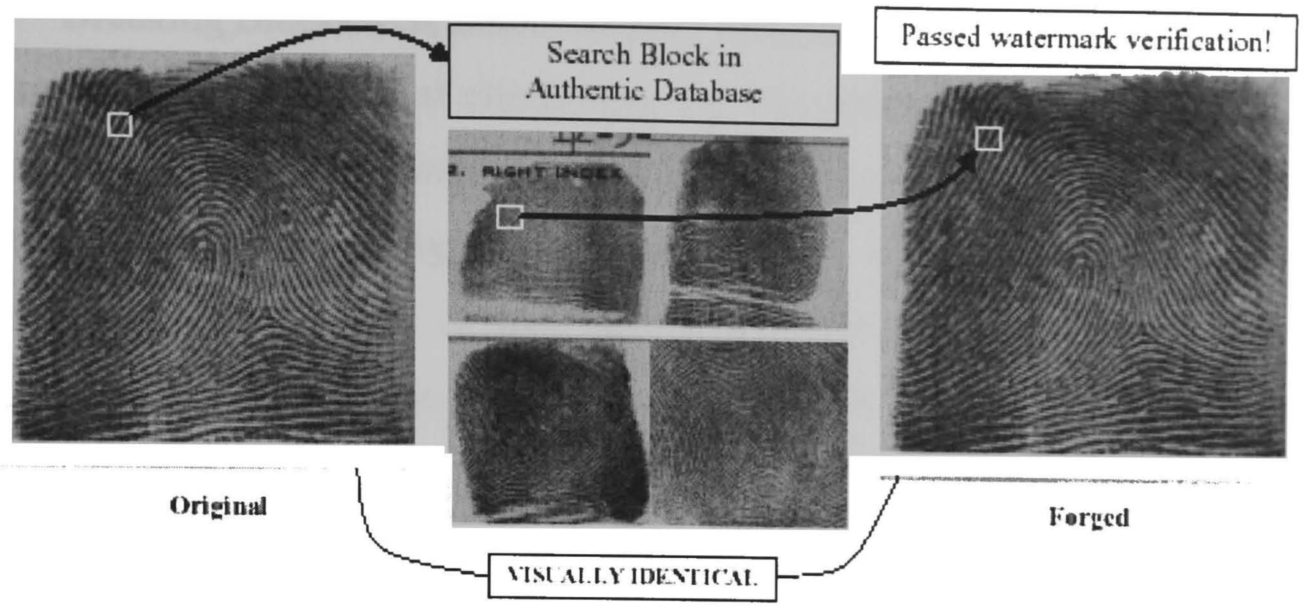

Search Block in Authentic Database
Passed watermark verification!
RIGHT INDEX
Original
Forged
VISUALLY IDENTICAL

Figure 5.2 **Vector quantization attack. The attacker approximates an image (on the left) by a collage of authentic blocks from watermarked images (center). The resulting image (right) is visually identical to the original and is deemed valid by the watermark detector.**

5.4 Countermeasures Against Counterfeiting Attack

In this section a number of modifications on Wong's scheme that have been proposed as countermeasures against the vector quantization attack are discussed.

- Increasing Block Dimensions

Vector quantization process depends on two key factors: the size and the number of image blocks in a codebook. Smaller size blocks can be approximated more accurately given a fixed size codebook. Similarly, better approximations can be obtained as the number of blocks in the codebook increases. Therefore, increasing the block dimensions used in the watermarking process can reduce the possibility of a reasonable forgery. Larger blocks also decrease the number of authentic blocks that can be obtained from one image and this will degrade the quality of forgery by reducing the codebook size.

This countermeasure, however, does not thwart the attack completely. If the set of watermarked images available to the attacker is quite large, reasonable forgeries can still be produced. Moreover, using larger and larger blocks also impairs the tamper localisation accuracy of the watermark.

- Breaking Block-Wise Independence: Neighbourhood Dependent Blocks

An alternative method of eliminating the VQ attack is to eliminate the block wise independence of the watermark. In particular, the signature embedded in block Xr may be calculated using a larger support Xr, which overlaps the neighbouring blocks. This technique is very similar to block chaining modes used in block encryption techniques (e.g., CBC mode in DES – see Menezes, Oorchoot et al. 1997). Using this scheme, a collage of individually watermarked blocks of an image is no longer authenticated by the watermarking extraction process because the larger support covering the neighbouring blocks is not preserved.

- Hierarchical Block-Based Watermarking

A technique that embeds and extracts a watermark in a multilevel hierarchy was proposed (Celik et al. 2002). On the lowest level, the image, X is partitioned into O x P non-overlapping blocks. At each successive level, the image is partitioned into blocks that in turn are composed of 2 x 2 blocks at the preceding level of the hierarchy.

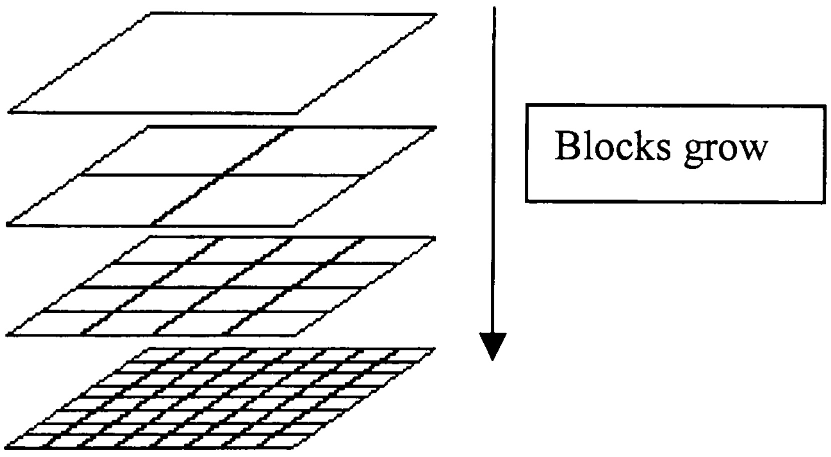


Figure 5.3 Partitioning of an image and the resulting four level hierarchical block structure

Although the method claimed it could eliminate the vulnerabilities of Wong's (1998) scheme to VQ attack, it is found that the method also compromises on the accuracy of localisation. For example, using an ultrasound image of size 800 x 600 pixels, the image will be partitioned, resulting in four level hierarchical block structure with the smallest block of 100 x 75 pixels.

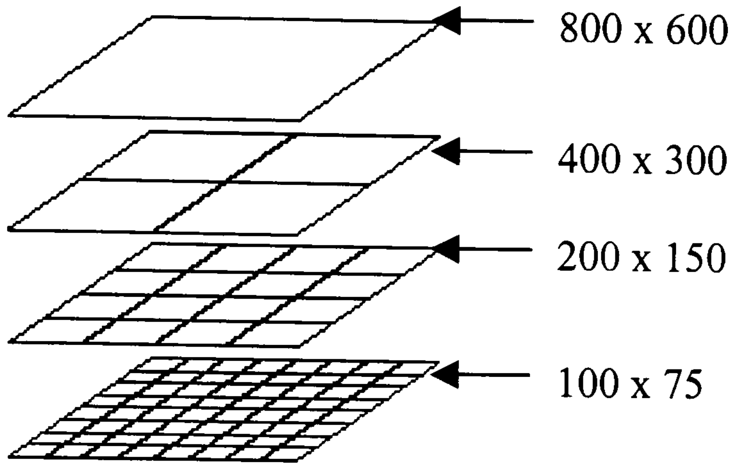


Figure 5.4 Partitioning of image size 800 x 600 pixels

5.5 Authentication Watermarking with Tamper Detection and Recovery (AW-TDR)

In this section, an efficient and effective digital watermarking method for image tamper detection and recovery is presented. The method is based on four concepts introduced from the literature: 1) block-based (Fridrich and Goljan 1999); 2) separating authentication bits and recovery bits (Lin and Chang 2001); 3) hierarchical (Celik et al 2002); and 4) average intensity as an image feature (Lou and Liu 2000). The method is efficient as it only uses simple operations such as parity check and comparison between average intensities. It is effective because the scheme inspects the image hierarchically with the inspection view increasing along with the hierarchy so that the accuracy of tamper localisation can be ensured. This scheme can perform both tamper detection and recovery for tampered images. Tamper detection is achieved through a block-based, inspection and recovery of a tampered block and relies on its feature information hidden in another block, which can be determined by a one-dimensional transformation.

5.5.1 Torus Automorphism

Torus automorphism is a kind of dynamic system. A dynamic system is a system whose states change with time t. When t is discreet, a dynamic system can be presented as iteration of a function f, $S_{t+1} = f(S_t)$, where $t \in \mathbf{Z} = \{0, 1, 2, 3, \dots\}$, S_t, S_{t+1} are the states at time t and $t+1$, respectively (Voyatzis and Pitas 1996a). A two-dimensional Torus automorphism can be considered as a permutation function or a spatial transformation of a plane region. This transformation can be performed using a 2 x 2 matrix A with constant elements. More specifically, a state S_{t+1} or a point (x_{i+1}, y_{i+1}) can be transformed from another state S_t or another point (x_i,y_i) by

$$A=\begin{pmatrix} a1 & a2 \\ a3 & a4 \end{pmatrix}, \begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = A\times\begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod N, \qquad (5.4)$$

where $a_i \in Z, |A|=1$, and A has eigenvalues $\lambda_{1,2} \in R-\{-1,0,1\}$, R is the set of rational numbers. The detailed characteristics of A are described in (Voyatzis and Pitas 1996b, Voyatzis and Pitas 1996a). A set of successive points $\{S_0, S_1, S_2, \ldots\}$, generated by equation (5.4) composes an orbit φ of the system and the initial point $S_0 = (x_0,y_0)$ classifies φ into two categories. When x_0 and/or y_0 are irrational, φ is infinite. When both x_0 and y_0 are rational, φ is chaotic and periodic at every R times, $S_R = S_0$. R is called the recurrence time. Voyatzis and Pitas (1996) presented a one-parameter, two dimensional, discrete Torus automorphism as in equation (5.5), for creating a unique and random mapping of the pixels within an image:

$$A=\begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix}, \quad \begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = A\times\begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod N, \qquad (5.5)$$

where $(x_i, y_i) \in [0, N-1]\times[0, N-1]$ and $k \in [0, N-1]$. The recurrence time R depends upon the parameters k, N, and the initial point (x_0,y_0). In most cases, R is equal to N-1 or N+1, when N is prime (Voyatzis and Pitas 1996b, Voyatzis and Pitas 1996a).

5.5.2 Watermark Embedding

The watermarking embedding procedure is described in this section. Each image is of size M x N pixels where M and N are assumed to be a multiple of six and the number of grey levels is 256.

- Preparation

We need to prepare a one to one block mapping sequence A → B→ C→ D → … → A for watermarking embedding, where each symbol denotes an individual block. The intensity feature of block A will be embedded in block B, and the intensity feature of block B will be embedded in block C, etc. Since the number of blocks in each dimension of most images can be hardly be a prime number, we cannot obtain a one to one mapping among the blocks by applying equation (5.5), based on the analysis in (Voyatzis and Pitas 1996b). Instead, a 1D transformation was used:

$$\vec{B} = [(k \times B) \bmod N_b] + 1, \qquad (5.6)$$

where $B, \vec{B}, k \in [1, N_b]$, k is a secret key (prime number), and N_b is the total number of blocks in the image.

The generation algorithm of the block-mapping sequence is as follows:

1. Divide the image into non-overlapping blocks of 6x6 pixels
2. Assign a unique and consecutive integer $B \in \{1,2,3,\ldots,N_b\}$ to each block from left to right and top to bottom, where N_b= (M/6) x (N/6)
3. Randomly pick a prime number $k \in [1, N_b]$
4. For each block number B, apply equation (5.6) to obtain $\vec{B}$, the number of its mapping block
5. Record all pairs of B and $\vec{B}$ to form the block mapping sequence

k	B	1	2	3	4	5	6	7	8	21	22	23	24
23	$\vec{B}$	24	7	30	13	36	19	2	25	4	27	10	33
26	$\vec{B}$	27	13	39	25	11	37	23	9	27	13	39	25

Table 5.1 Mapping of blocks with k=23,26 and Nb=40

Note that the secret key, k, must be a prime in order to obtain a one to one mapping; otherwise, the period is less than N_b and a one to many mapping may occur. Table 5.1 lists some parts of the mapping sequence generated with Nb=40, k=23 and 26 respectively. In this table, $\vec{B}$ starts to repeat at B=21 when k=26, which is not a prime.

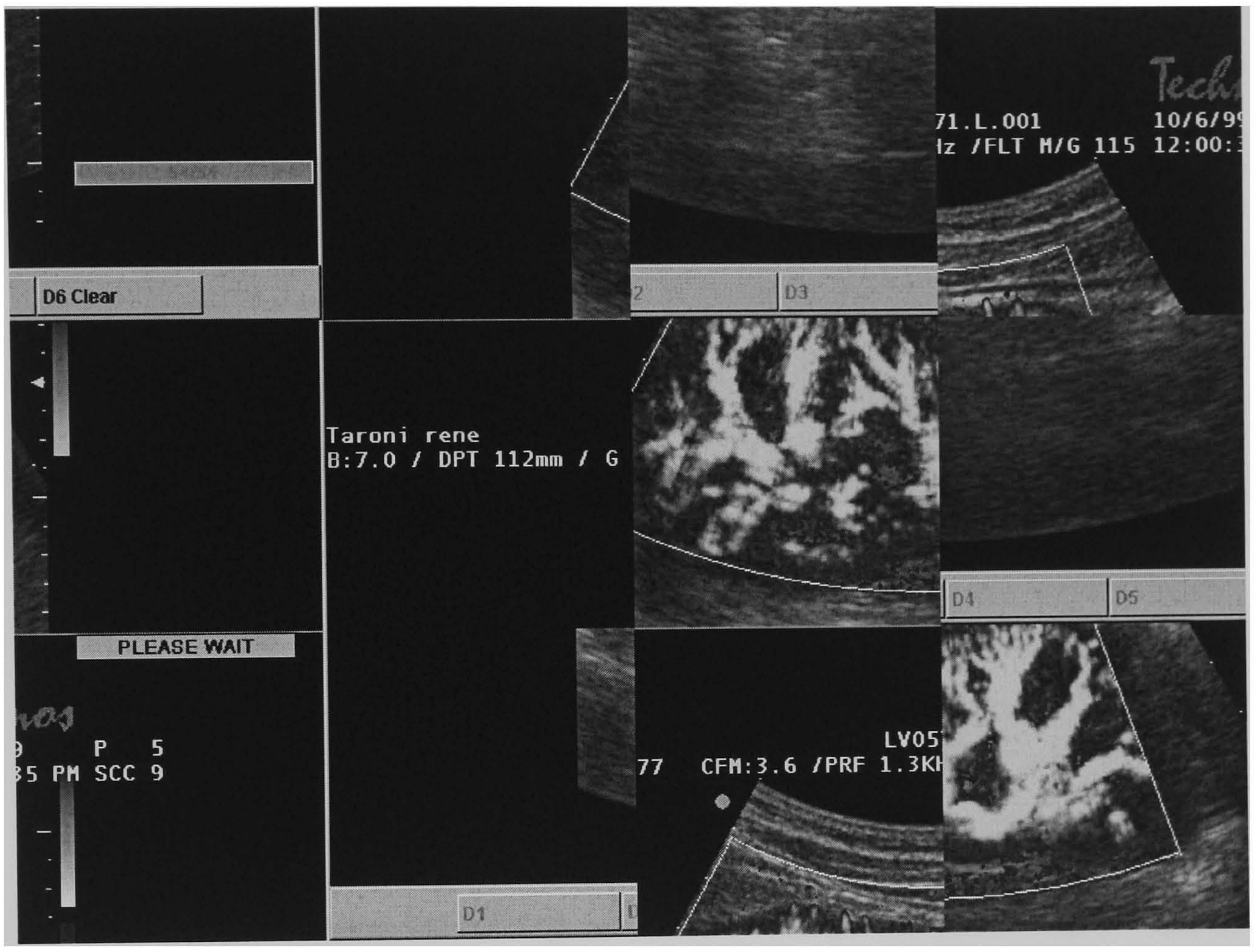


Figure 5.5 Image mapping using toral automorphism. Blocksize=200 k= 5

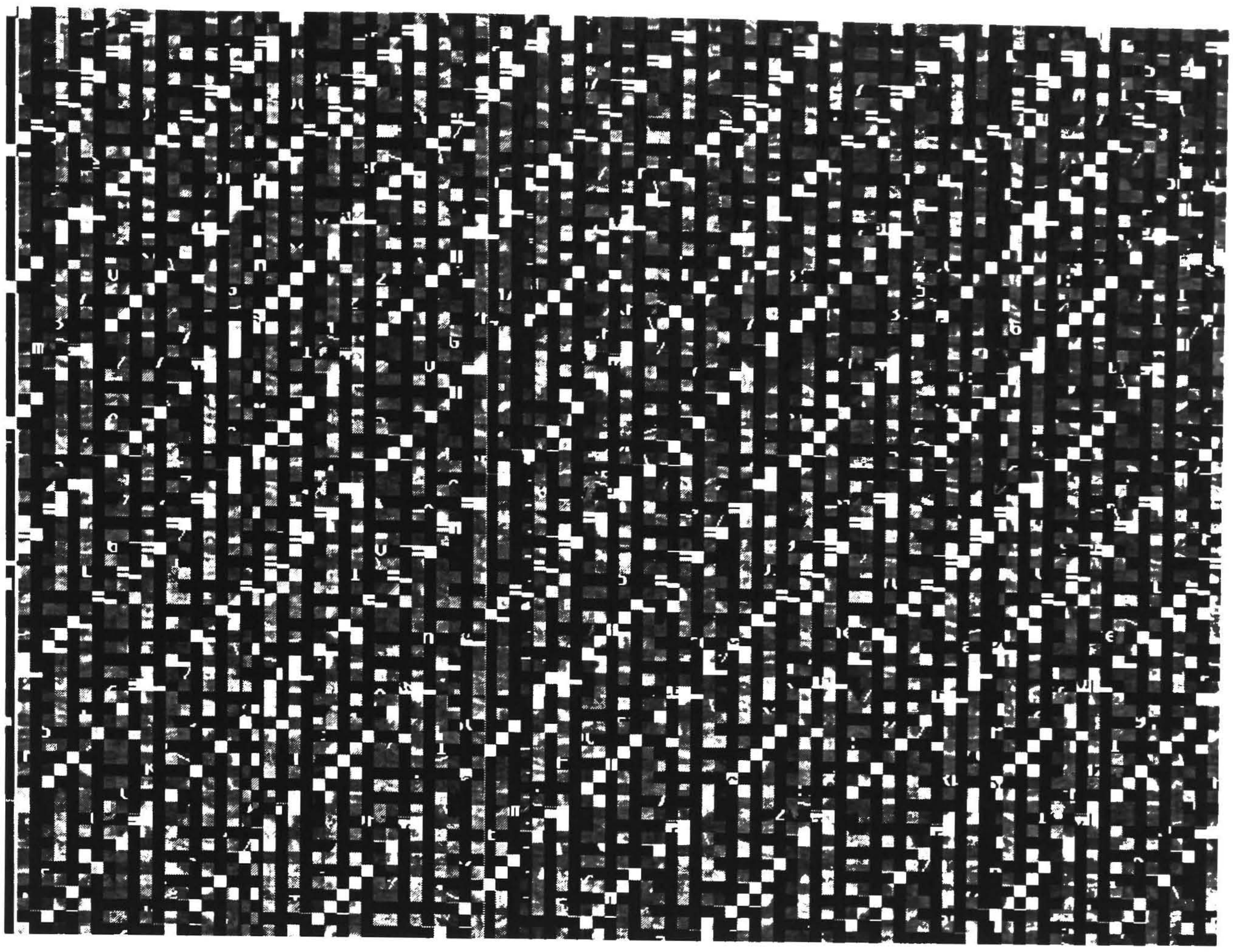


Figure 5.6 image mapping using toral automorphism. Blocksize=8 k= 3739

Figure 5.5 and 5.6 shows an 800x600 ultrasound image divided into equal size blocks and mapped using toral automorphism.

- Authentication watermark and recovery watermark generation

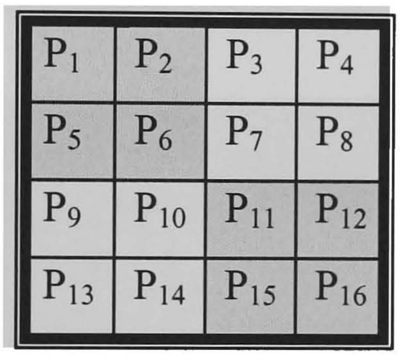
In the schemes proposed by Wong (1998) and Celik et al. (2002) a signature was generated for each block in order to localise tamper. Signature generation is computationally expensive and requires more bits for embedding, thus it will have an effect on the quality of the watermarked image.

In this section a case of using intensity average comparisons and parity bits as the authentication watermark is presented. To localise tamper in a block, the watermark needs to be embedded directly into that block. If a block is being tampered locally, the intensities of the pixels involved will be changed. This will also change the average intensity of the block concerned. To ensure that this is not changed, a parity check will be used. However, a parity check alone will not guarantee that the block has not been changed, because local tampering usually causes burst error (Cox et al. 2002), meaning that if more than one bit has been changed, a parity check is no longer useful. Using ECC will help solve this issue, but again more watermark bits will be needed. To overcome this, the intensity comparison is used as another guard if a parity check fails. This feature will also be used to break block wise independent. To break block wise independent, the intensity of the block is compared to the intensity of a larger block. Let B denote the bigger block (figure 5.7) and the smaller or sub block as B$_s$, then the average intensity of B is

$$Avg\_B = \frac{(P_1 + P_2 + P_3 + \ldots + P_{15} + P_{16})}{16} \tag{5.7}$$

and the average intensity of sub block is

$$Avg\_B_s = \frac{(P_1 + P_2 + P_5 + P_6)}{4} \tag{5.8}$$



P_1	P_2	P_3	P_4
P_5	P_6	P_7	P_8
P_9	P_{10}	P_{11}	P_{12}
P_{13}	P_{14}	P_{15}	P_{16}

Figure 5.7 A 4x4 Block B

The intensity of each sub block will be used as the recovery watermark, and will be embedded in a block mapped by equation 5.6. This is to ensure that if the block is tampered with, the recovery bits will be highly likely to be available. In order to consider the block size suitable for recovery, the average intensities of 4x4, 3x3 and 2x2 blocks of the whole image were created to see the visual effect for each block size and the results of the signature image are presented in figure 5.6, 5.7 and 5.8 respectively. The 4x4 signature image loses fine details with clearly visible block effect. The 3x3 signature image has better quality, with fine details and less visible block effect. The 2x2 signature is the best without losing any fine details and no visible block effect.

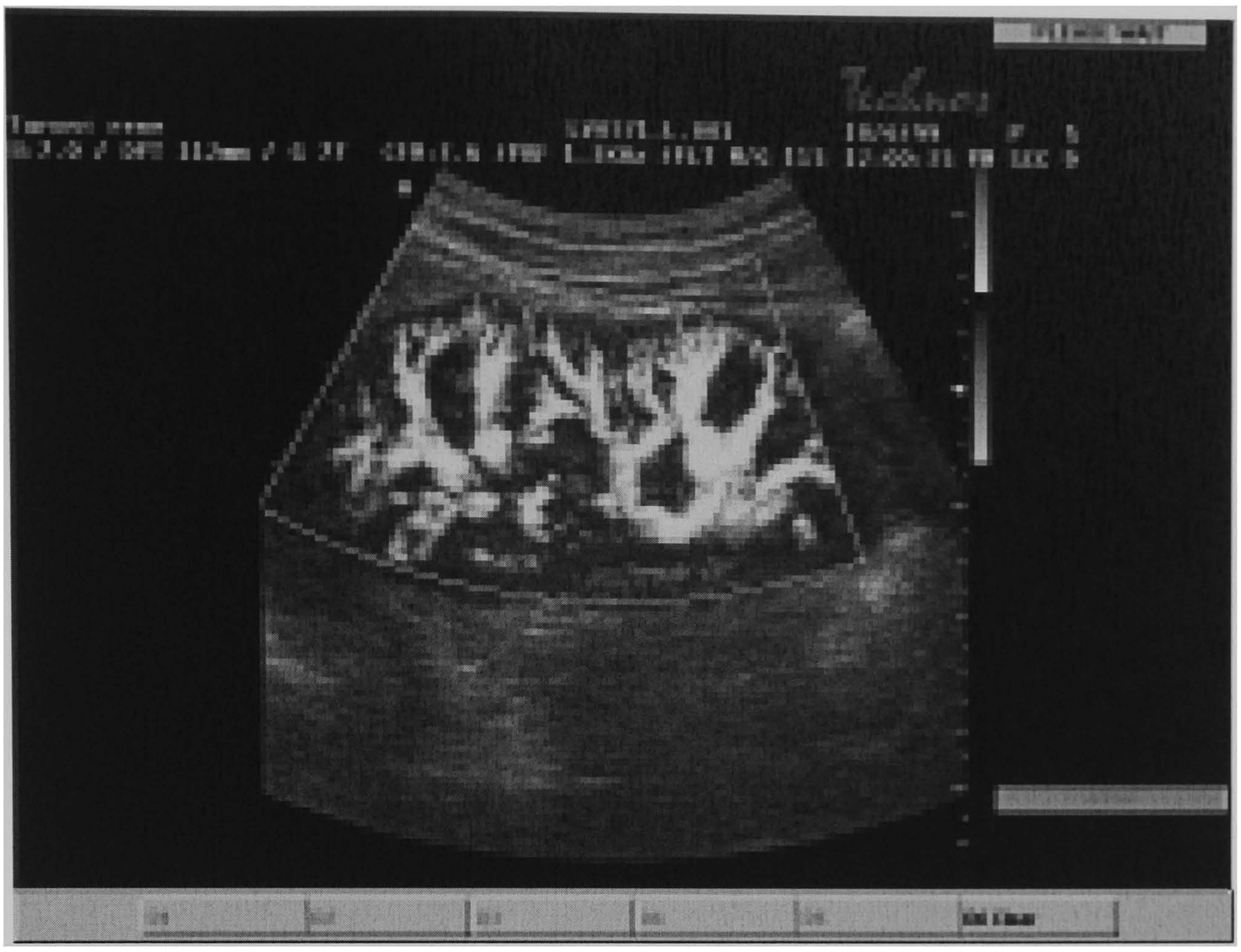


Figure 5.8 Signature image using 4x4 block.

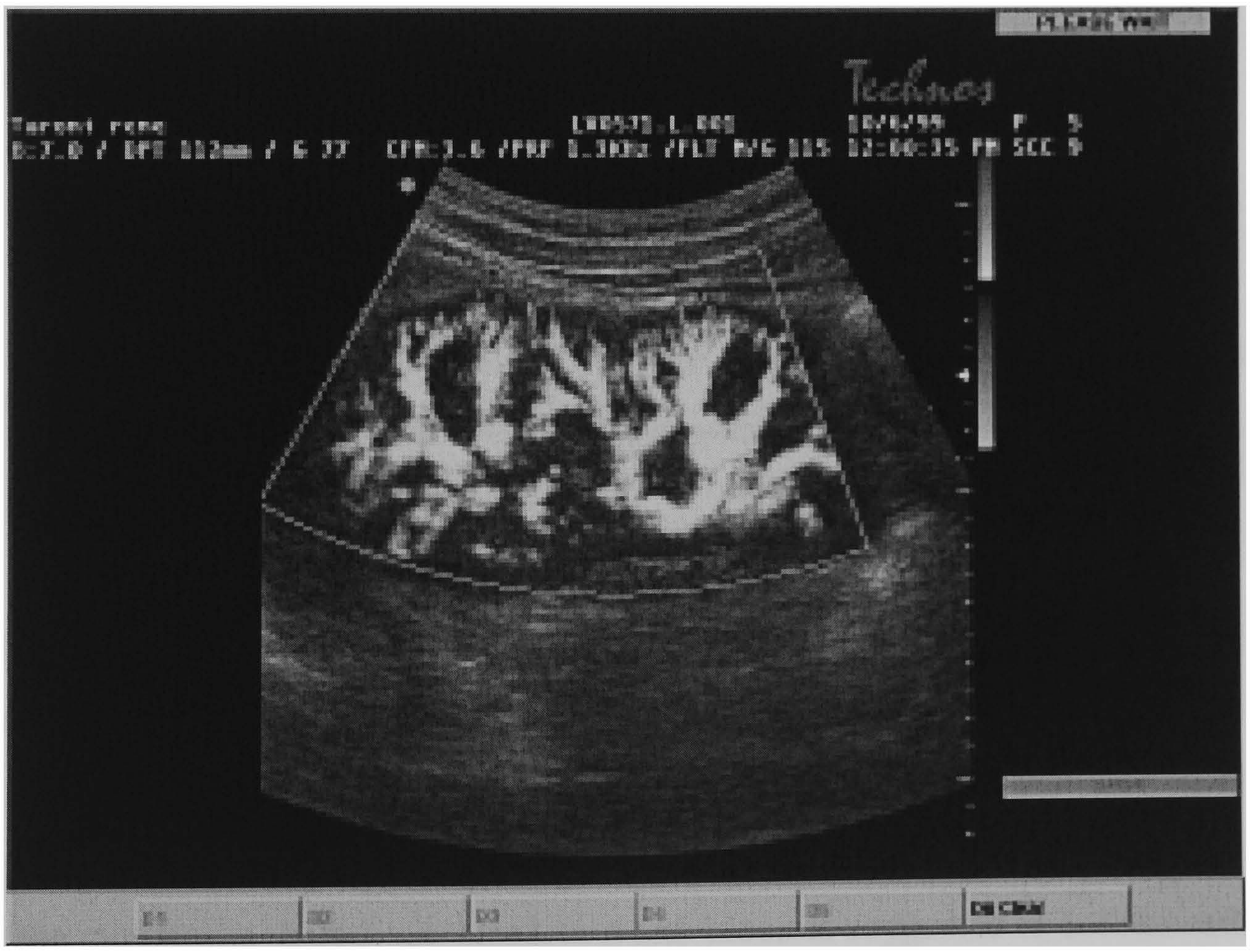


Figure 5.9. Signature image using 3x3 block

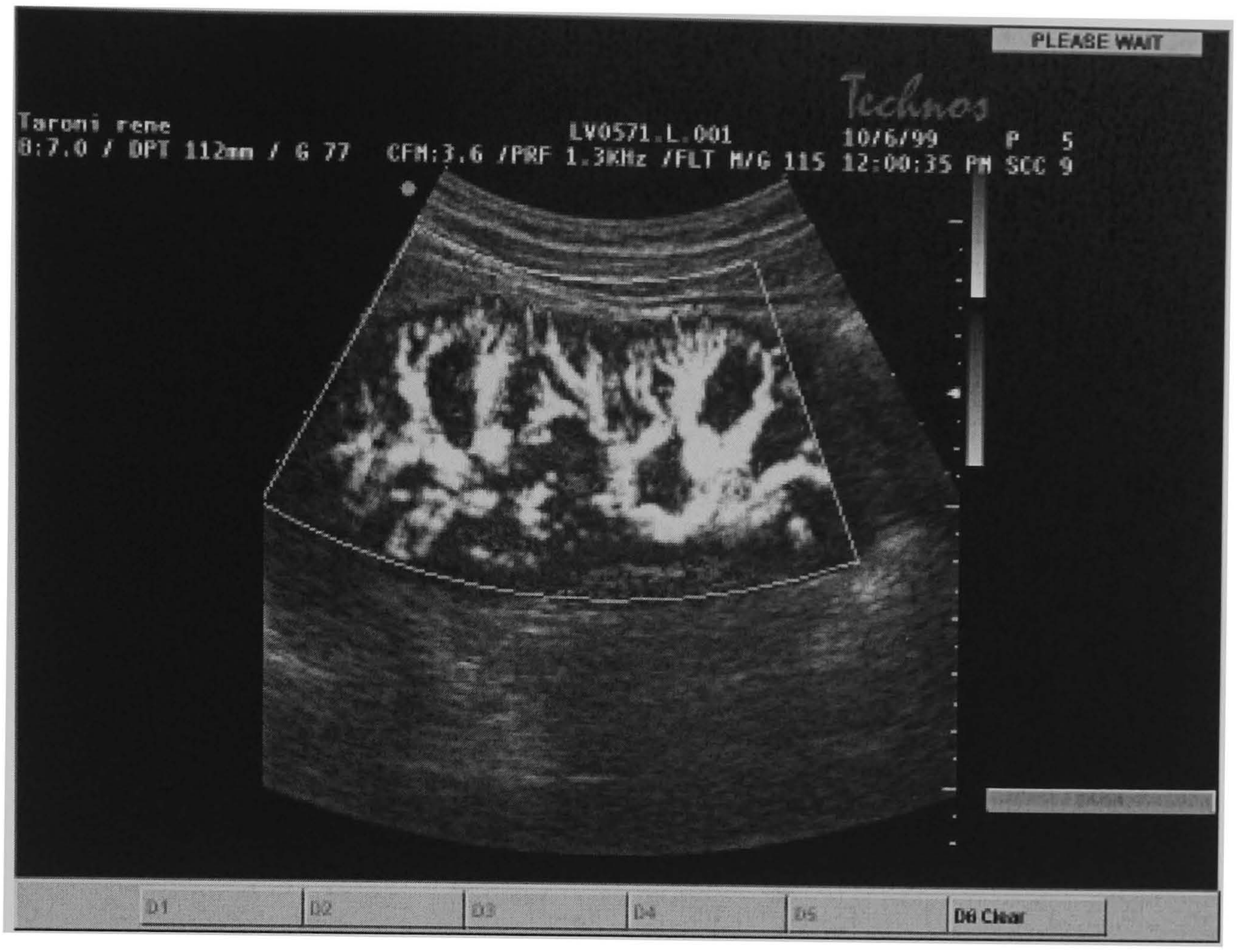


Figure 5.10. Signature image using 2x2 block. Quality is good. No visual block effect. A good candidate for recovery.

The choice of which signature image to use will depend on:

1. How many LSBs will be used, which is the answer to how much degradation is allowed for the watermark.
2. How will the recovered image be used? Will it be considered as authentic? If it is not, will it be used as an indication of the location and the nature of the tampering?

LSB is suggested, to minimise the degradation as medical images are very strict with the quality. The recovered image, however, will not be considered authentic and will not be used for any clinical purposes. One possibility for the purpose of recovery is to help in the investigation to find the motive and the person responsible for the tampering. A 3x3 sub block in a 6x6 block is suggested to accommodate two authentication bits and seven recovery bits to be embedded in the LSB of each pixel.

- Embedding

For each block B of 6x6 pixels, divide it into four sub-blocks of 3x3 pixels. The watermark in each sub-block is a 3-tuple (v, p, r), where both v and p are 1-bit authentication watermark, and r is a 7-bit recovery watermark for the corresponding sub-block within block A mapped to B. The following algorithm describes how the 3-tuple watermark of each sub-block is generated and embedded:

1. Set the LSB of each pixel within the block to zero and compute the average intensity of the block and each of its four sub-blocks, denoted by avg_B and avg_B_s, respectively.

2. Generate the authentication watermark, v, of each sub-block as:

$$v = \begin{cases} 1 & if\, avg\_Bs \geq avg\_B, \\ 0 & otherwise, \end{cases} \tag{5.9}$$

3. Generate the parity check bit, p, of each sub-block as :

$$p = \begin{cases} 1 & if\, num\, is\, odd, \\ 0 & otherwise, \end{cases} \tag{5.10}$$

   where num is the total number of 1s in the seven MSBs of avg_B_s.

4. From the mapping sequence generated in the preparation step, obtain block A whose recovery information will be stored in block B.
5. Compute the average intensity of each corresponding sub-block As within A, and denote it avg_A_s.
6. Obtain the recovery intensity, r, of A_s by taking the seven MSBs in avg_A_s.
7. Embed the 3-tuple watermark (v, p, r), 9 bits in all, onto the LSB of of each pixel in Bs.

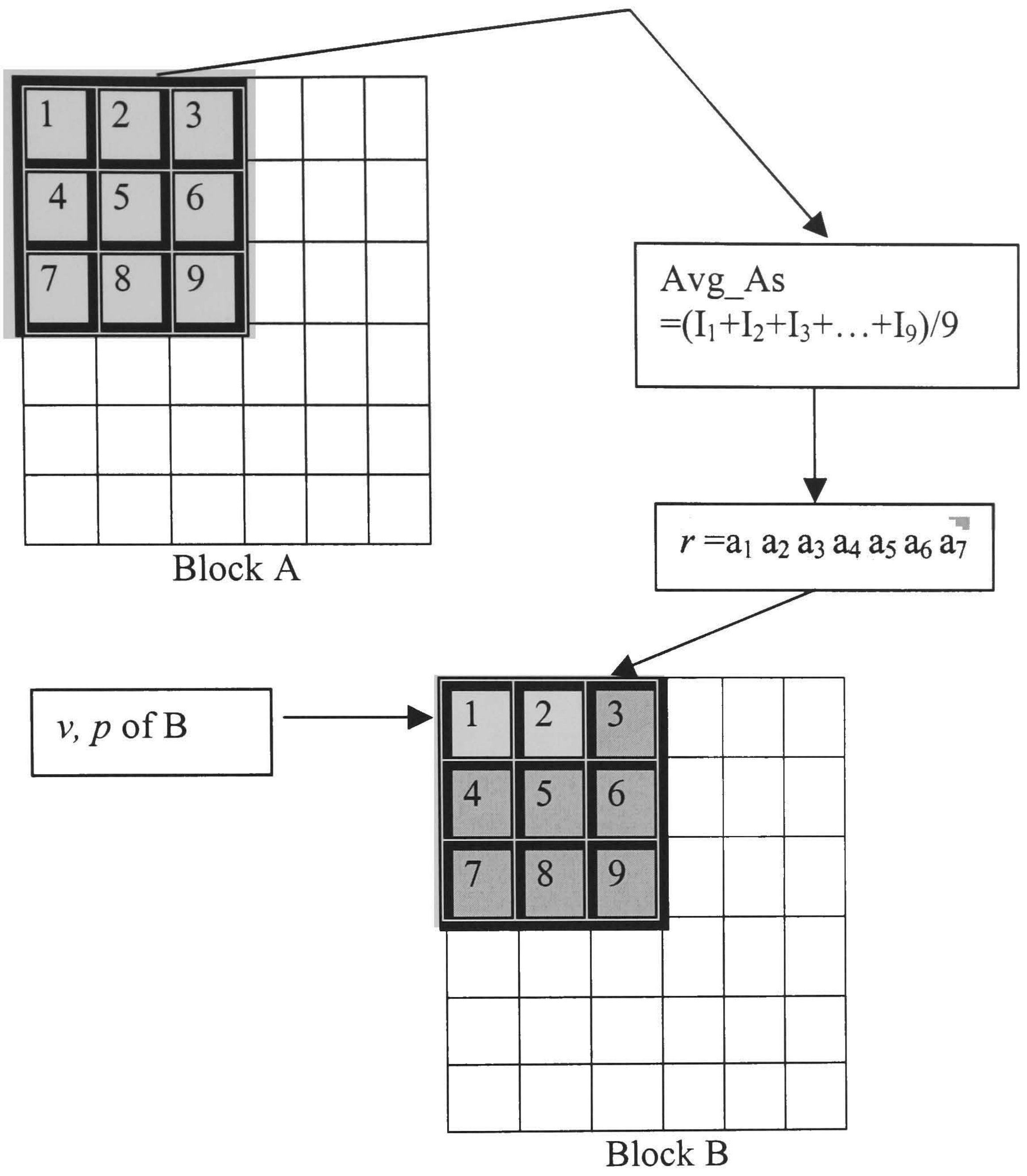

1 2 3
4 5 6
7 8 9
Block A
Avg_As
$=(I_1+I_2+I_3+\ldots+I_9)/9$
$r = a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7$
v, p of B
1 2 3
4 5 6
7 8 9
Block B

Figure 5.11(a) Watermark generation and embedding location

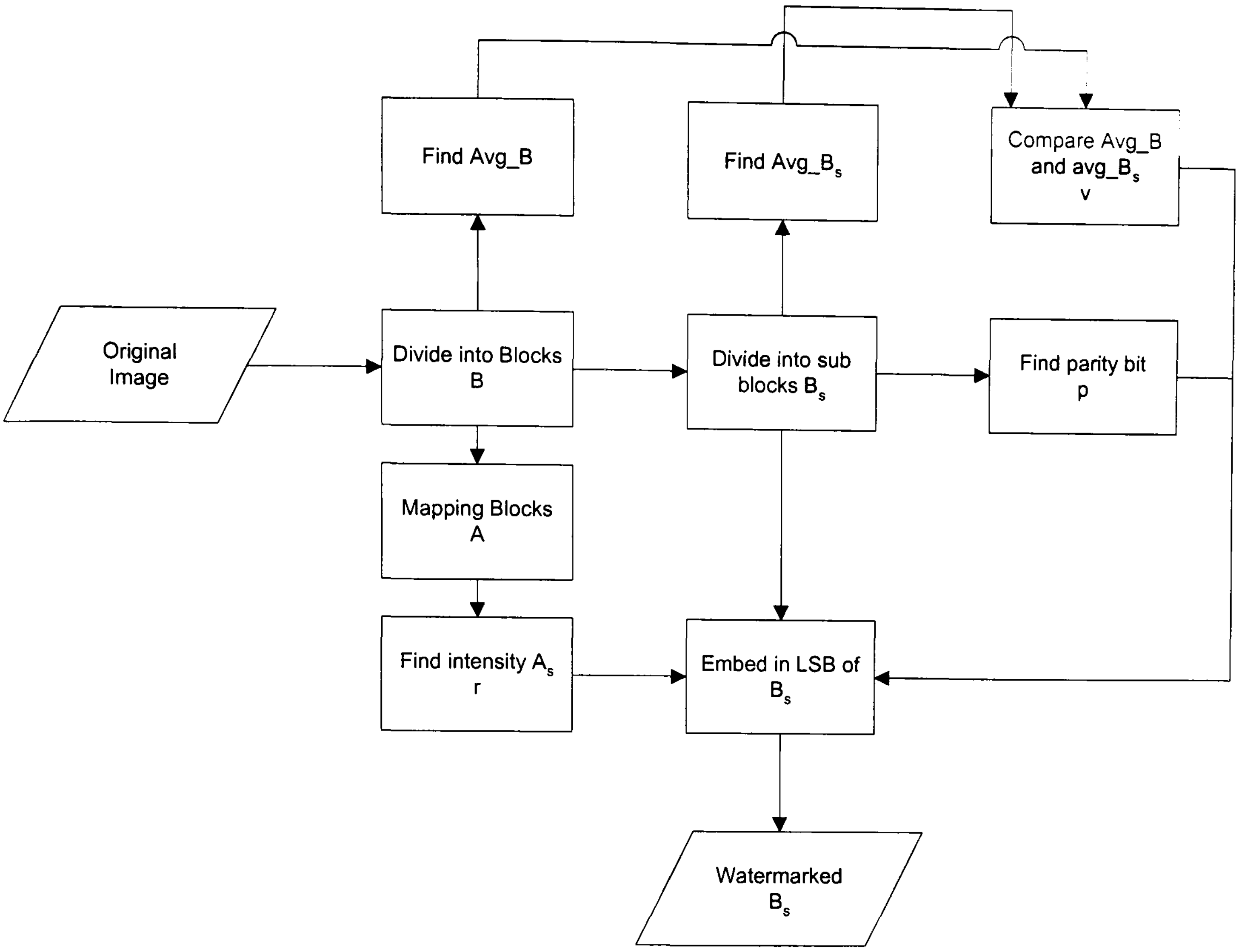


Figure 5.11(b) AW-TDR embedding scheme

5.5.3 Tamper detection

The test image is first divided into non-overlapping blocks of 6x6 pixels, as in the watermarking embedding process. For each block denoted as $\vec{B}$, the LSBs of each pixel in $\vec{B}$ were set to zero and compute its average intensity, denoted as avg_$\vec{B}$. A 2-level detection is then performed. In level-1 detection, each 3x3 sub-block within one block is examined. In level-2 detection, a 6x6 block is treated as one unit. Level-3 detection is for VQ attack resilience only. The procedure of our hierarchical tamper detection scheme is described in the following:

- Level-1 detection.

For each sub-block $\vec{B}$s of 3x3 pixels within the block $\vec{B}$, perform the following steps:

1. Extract v and p from $\vec{B}_s$.

2. Set the LSBs of each pixel within each $\vec{B}_s$ to zero and compute the average intensity for each sub-block $\vec{B}_s$, denoted as avg_$\vec{B}$ s.
3. Count the total number of 1s in avg_$\vec{B}_s$ and denote it as P_s.
4. Set the parity check bit p' of $\vec{B}_s$ to 1 if P_s is odd, otherwise, set it to 0.
5. Compare p' with p. If they are not equal, mark $\vec{B}_s$ as tampered and complete the detection for $\vec{B}_s$.
6. Set the algebraic relation v'=1 if avg_$\vec{B}_s$>=avg_$\vec{B}$, otherwise, set it to 0.
7. Compare v' with v. If they are not equal, mark $\vec{B}_s$ as tampered and complete the detection for $\vec{B}_s$; otherwise mark it valid.

- Level-2 detection.

For each block of size 6x6 pixels, mark this block tampered if any of its sub-blocks is marked tampered; otherwise mark it valid.

- Level-3 detection.

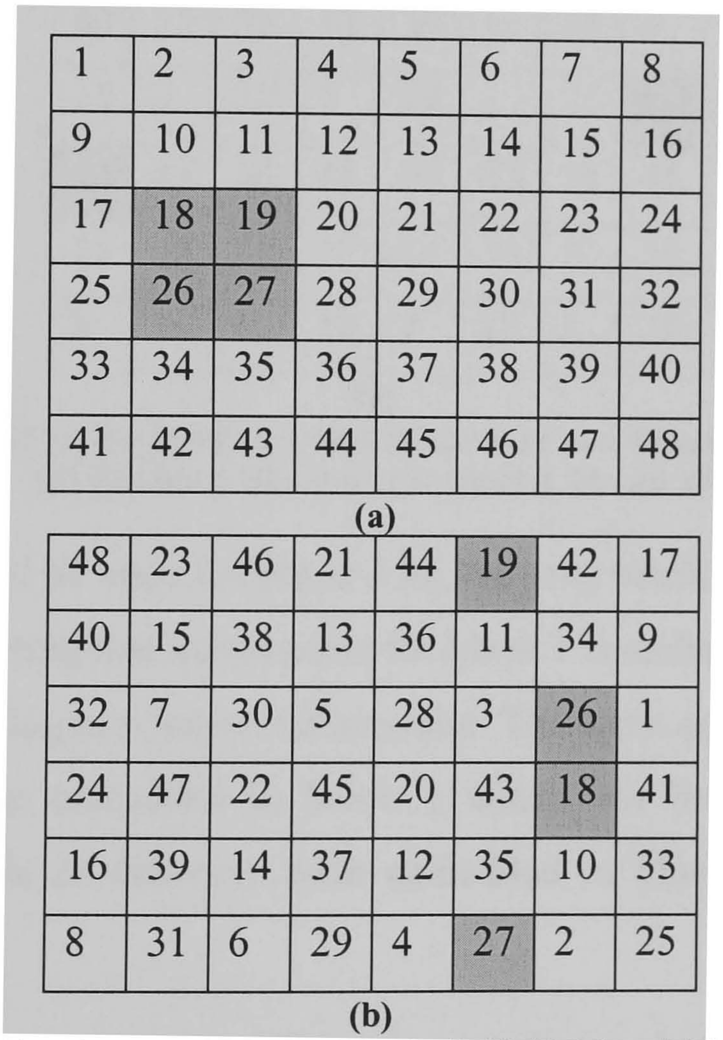
For each valid block $\vec{B}$ of size 6x6 pixels, perform the following steps:

1. Find the block number of block C, where block C is the one in which the intensity feature of block $\vec{B}$ is embedded.
2. Locate block C.
3. If block C is marked tampered, assume block $\vec{B}$ is valid and complete the test.
4. If block C is valid, perform the following steps:
   a. Obtain the 7-bit should-be intensity of each $\vec{B}_s$ by extracting the LSBs from each pixels in the corresponding block within block C, padding one zero to the end to make an 8-bit value.
   b. Compare with avg_$\vec{B}$ s and mark $\vec{B}$ tampered if they are different.

5.5.4 Image Recovery

After the detection stage, all the blocks are marked either valid or tampered. Only the tampered blocks are recovered and the valid blocks are left as they are. For convenience, we call the tampered block, block B and the block embedded with its intensity, block C. The restoration procedure for each tampered block is described as follows:

1. Calculate the block number for block C.
2. Locate block C
3. Obtain the 7-bit intensity of each sub-block within block B, padding one zero to the end to make an 8-bit value.
4. Replace the new intensity of each pixel within the sub-block with this new 8-bit intensity.
5. Repeat step 3 and 4 for all sub-blocks within block B.



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48

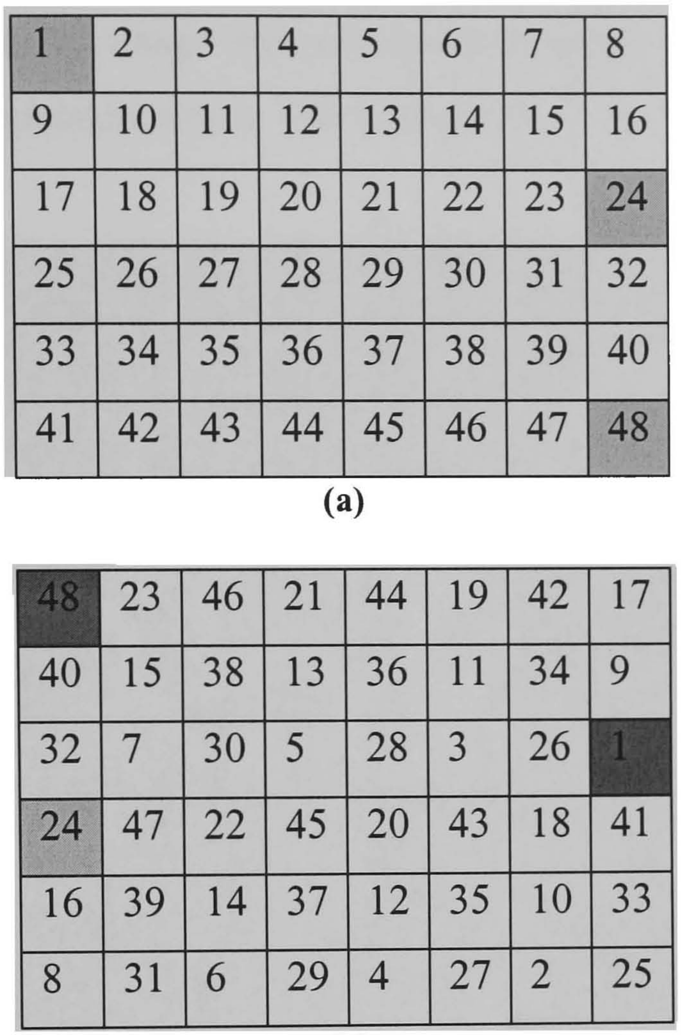
(a)

48	23	46	21	44	19	42	17
40	15	38	13	36	11	34	9
32	7	30	5	28	3	26	1
24	47	22	45	20	43	18	41
16	39	14	37	12	35	10	33
8	31	6	29	4	27	2	25

(b)

Figure 5.12. (a) An 8x6 block with block 18,19,26 and 27 tampered, (b) Recovery bits location

Figure 5.12(a) shows an 8x6 block and each block is given a number from 1 to 48. By using the transformation given by equation 5.3, with k=23, the transformation is given in figure 5.12(b). If, for example, blocks 18, 19, 26 and 27 were tampered with, all blocks will be recovered since from the mapping block, as the recovery bits are stored in blocks 6, 23, 31 and 46 respectively.



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48

(a)

48	23	46	21	44	19	42	17
40	15	38	13	36	11	34	9
32	7	30	5	28	3	26	1
24	47	22	45	20	43	18	41
16	39	14	37	12	35	10	33
8	31	6	29	4	27	2	25

(b)

Figure 5.13 (a) An 8x6 block with blocks 1,24 and 48 are tampered, (b) Recovery bits stored in block 1,24 and 25

If three blocks 1, 24 and 48 were tampered with, the only block that will be recovered is block 24. The reason being that information for block 1 is embedded in block 24, which is tampered with resulting in a loss of information. The same applies to block 48, where the recovery bits were embedded in block 1 which has been tampered with. The recovery bits for block 24 however were embedded in block 25 that has not been tampered with.

5.5.5 Experimental Results

- Missing detection

In evaluating the proposed authentication watermarking with tamper detection and recovery (AW-TDR), different manipulations on an ultrasound image, two fingerprint images and a military image were tested to obtain the miss detection rate for level-1 and level-2 detection.

The watermarked ultrasound image was manipulated using cloning tool from Adobe Photoshop CS. The manipulated area is ~30 x 50 pixels.

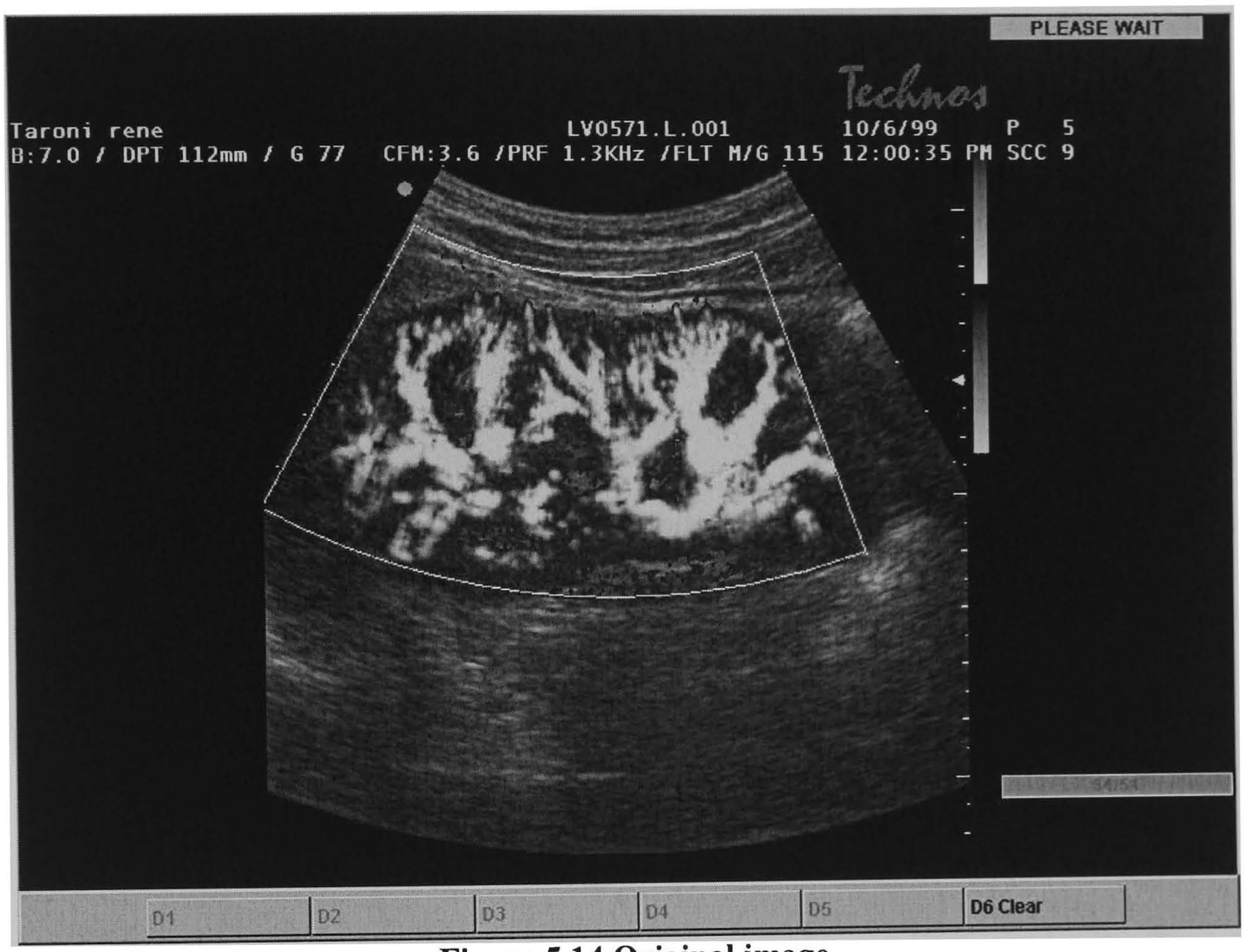


Figure 5.14 Original image

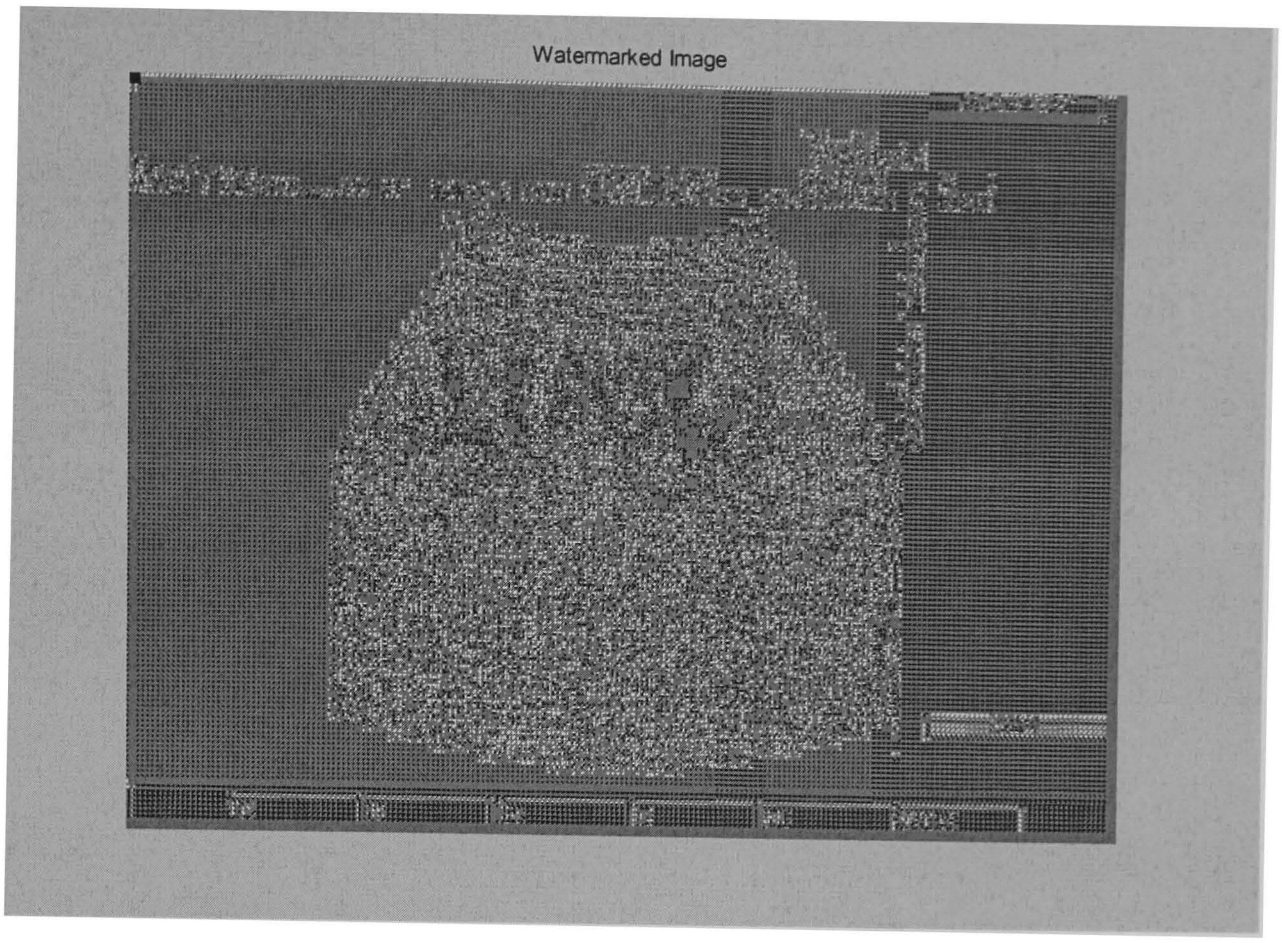


Figure 5.15 Watermark embedded PSNR = 54.1483 dB

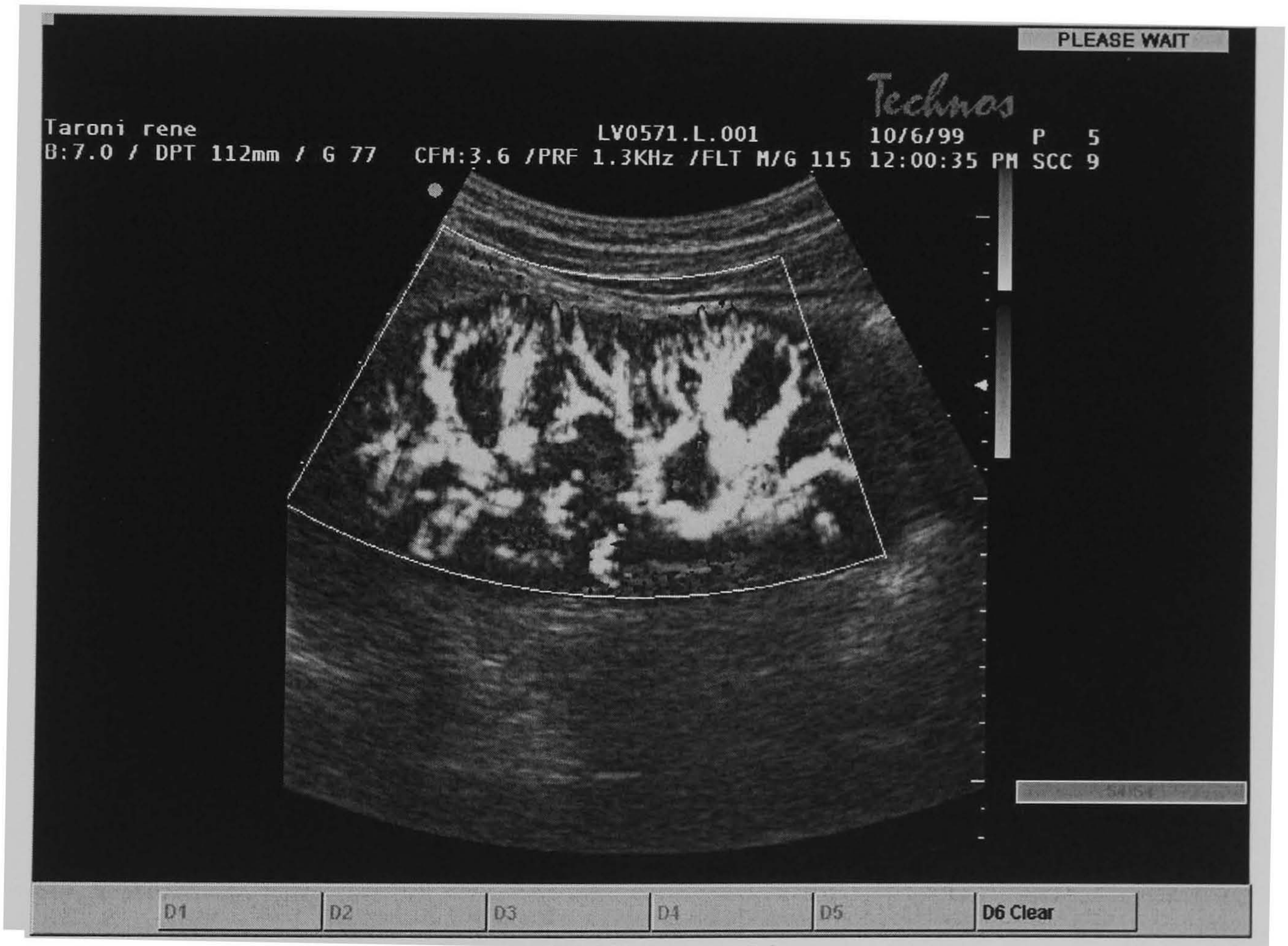


Figure 5.16 Tampered image

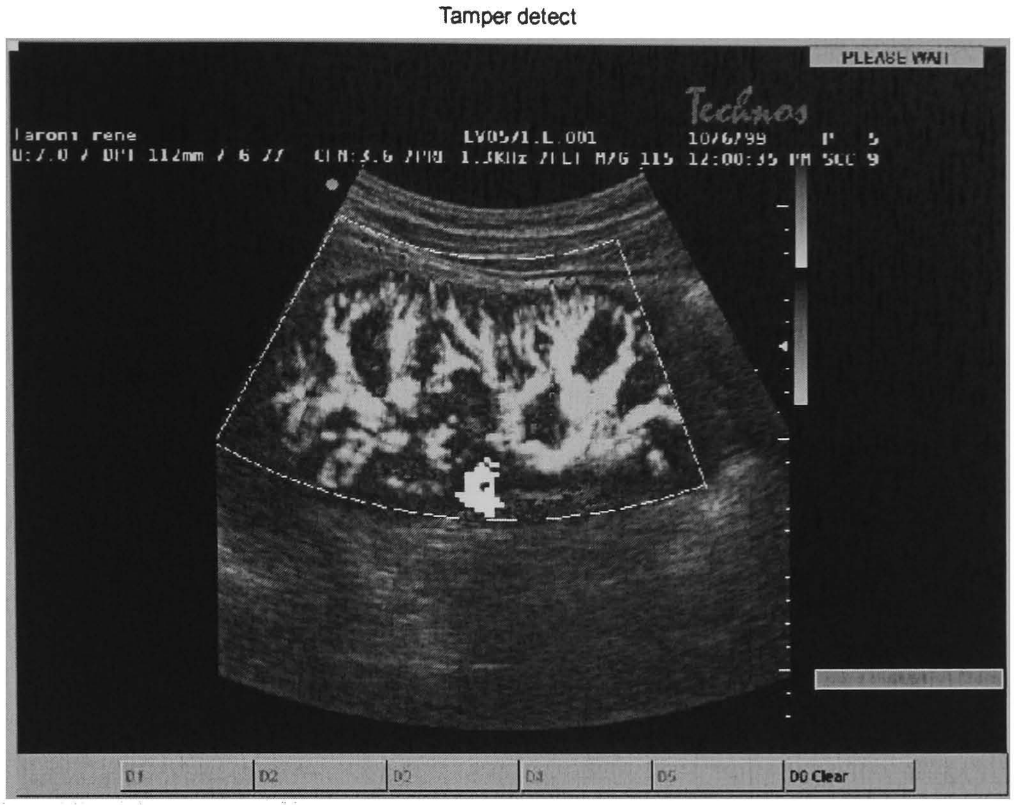


Figure 5.17 Level 1 detection with some areas undetected

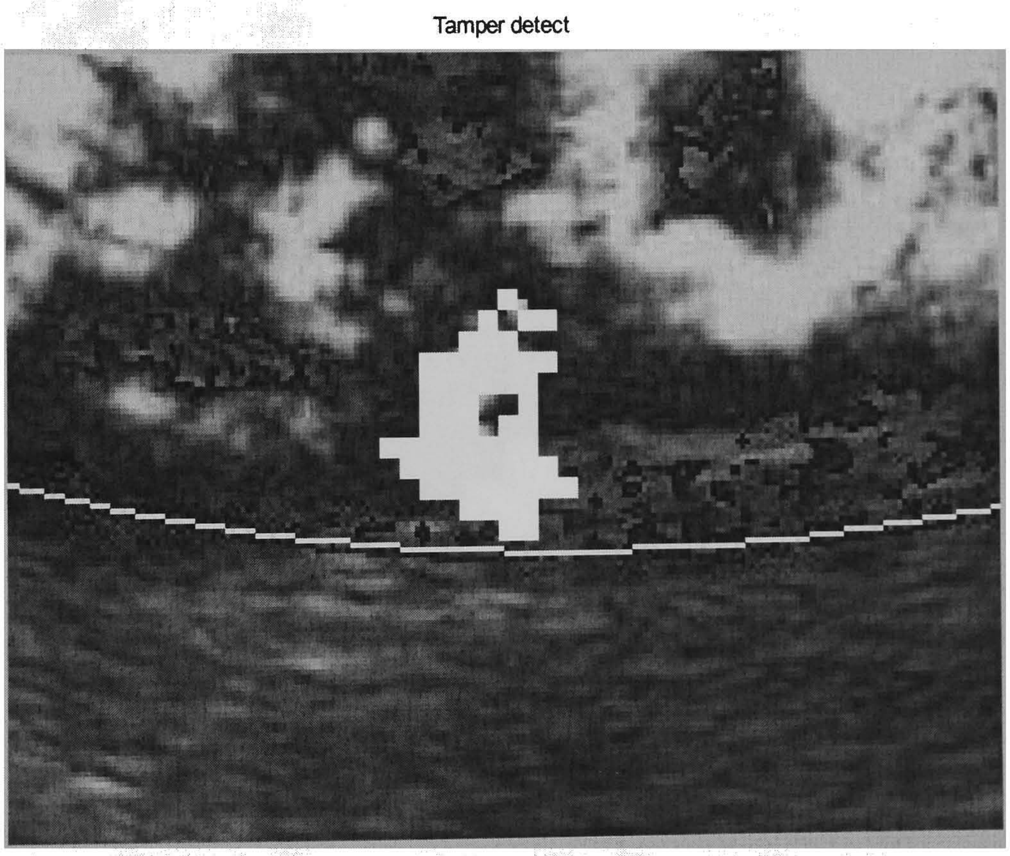


Figure 5.18 Some areas undetected magnified

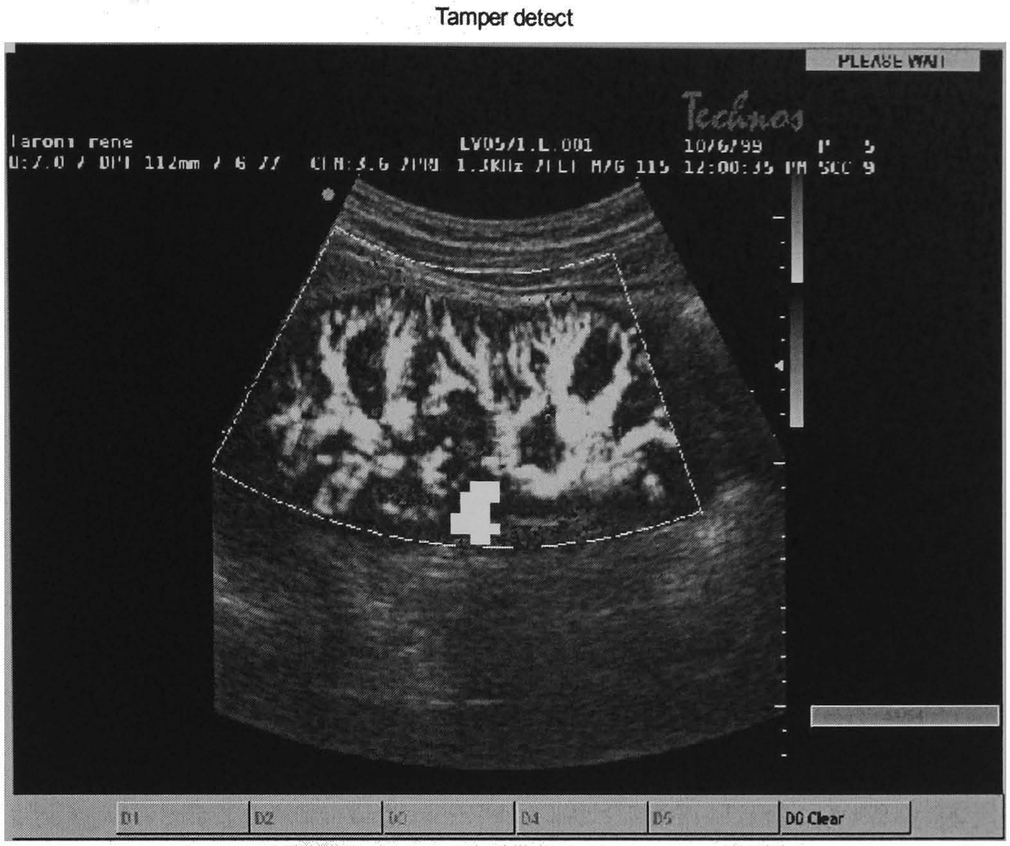


Figure 5.19 level 2 detection

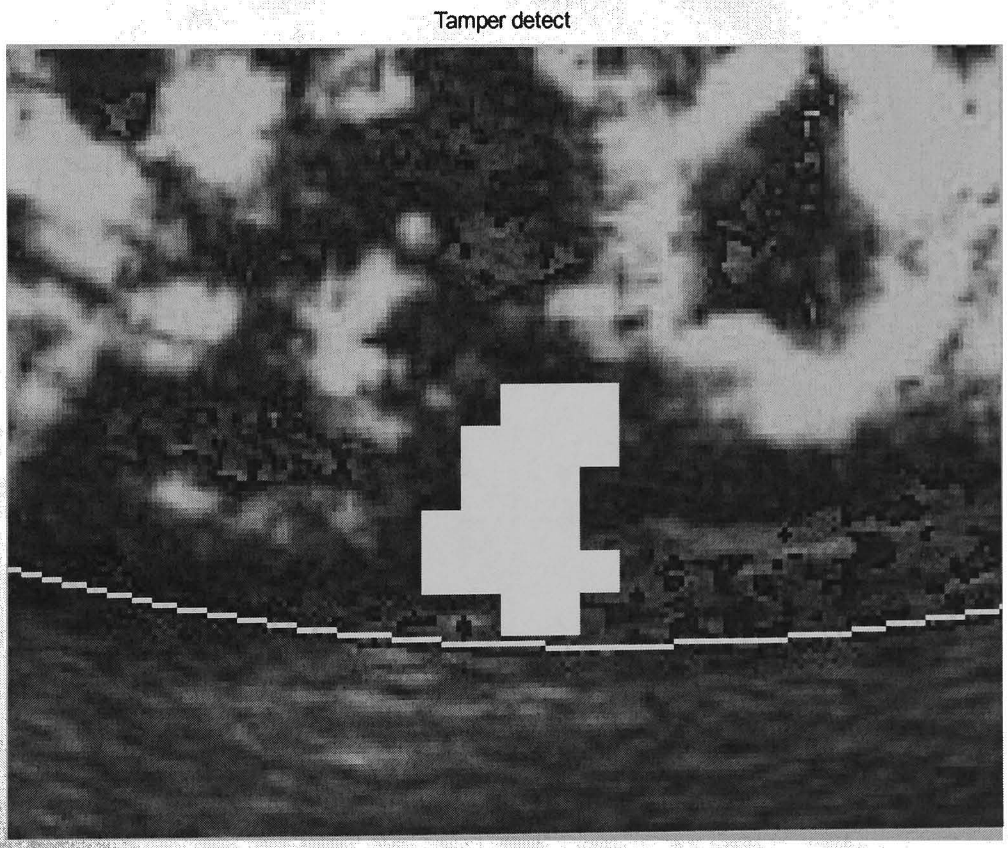


Figure 5.20. Magnified Level 2 detection

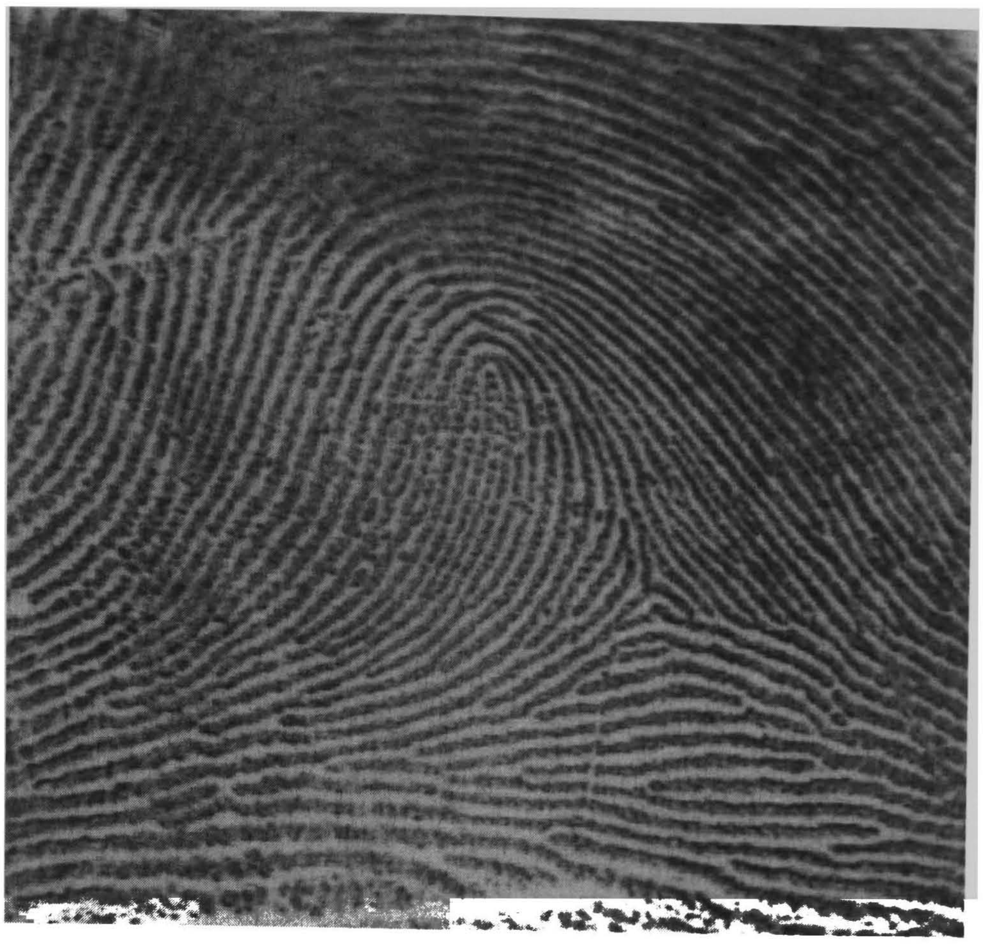


Figure 5.21. Original fingerprint1 (from National Institute of Science and Technology [NIST] Science and Technical database http://www.nist.gov/srd/nistsd4.htm)

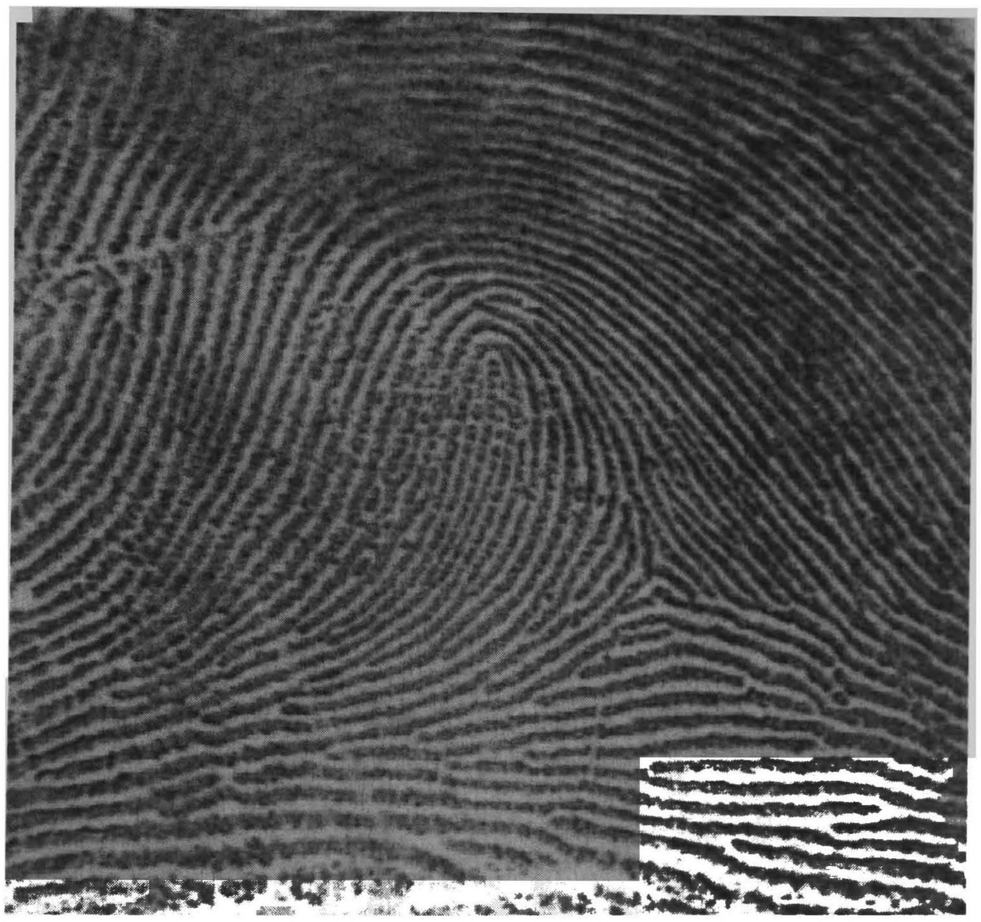


Figure 5.22. Watermarked fingerprint1 PSNR = 54.5262 dB

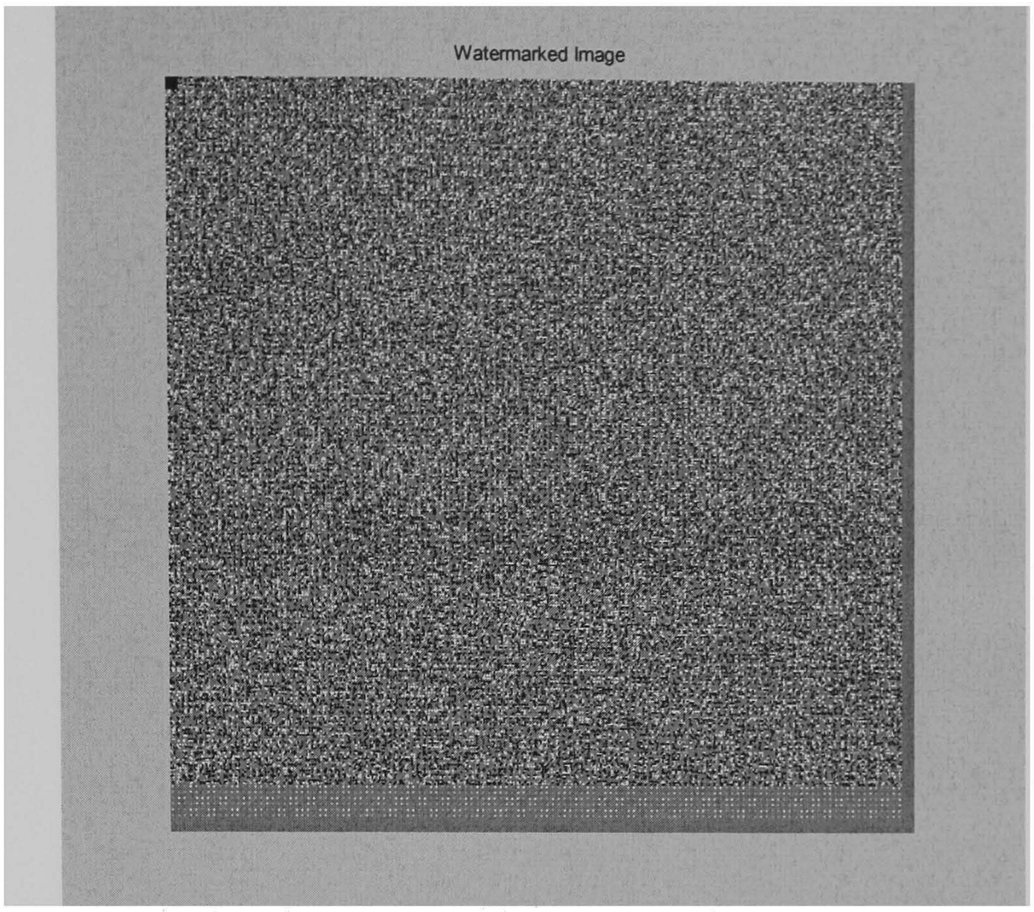


Figure 5.23. Watermark embedded in fingerprint1

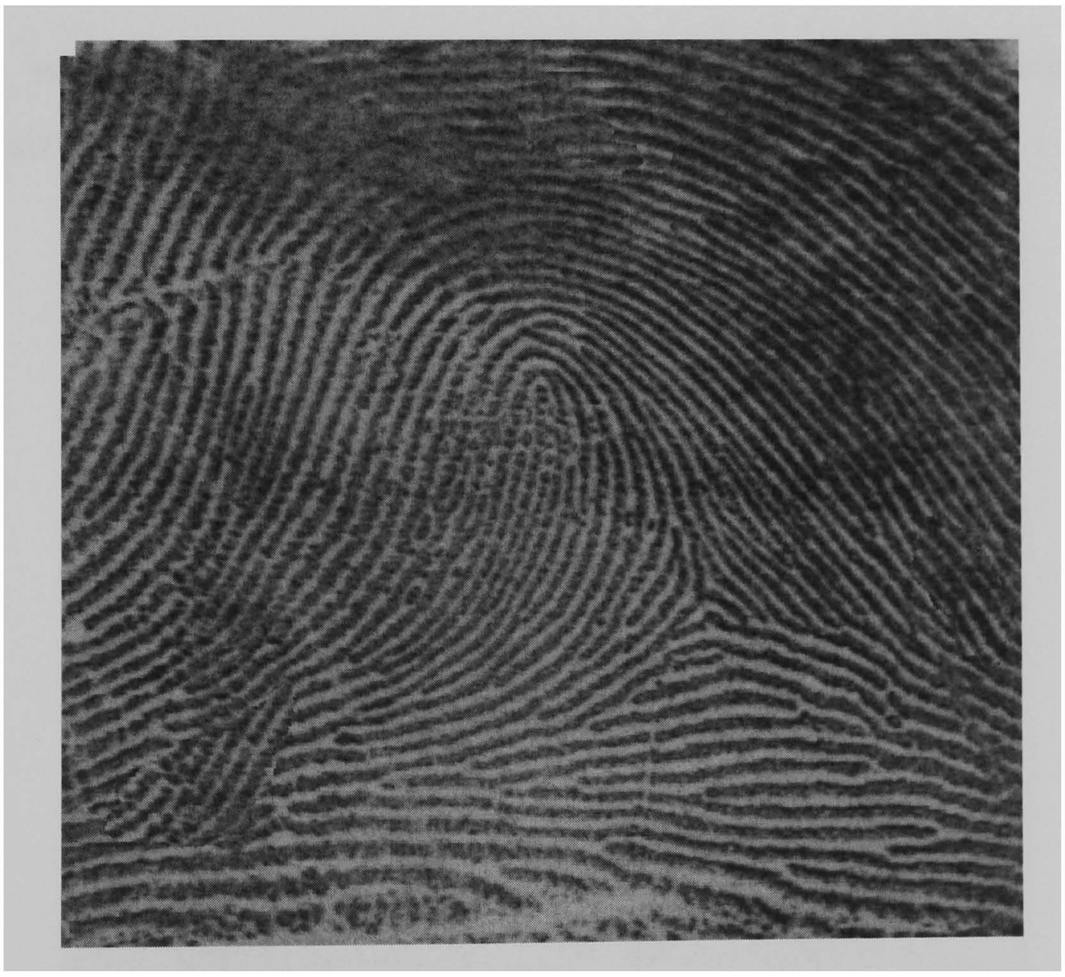


Figure 5.24. Tampered watermarked fingerprint1

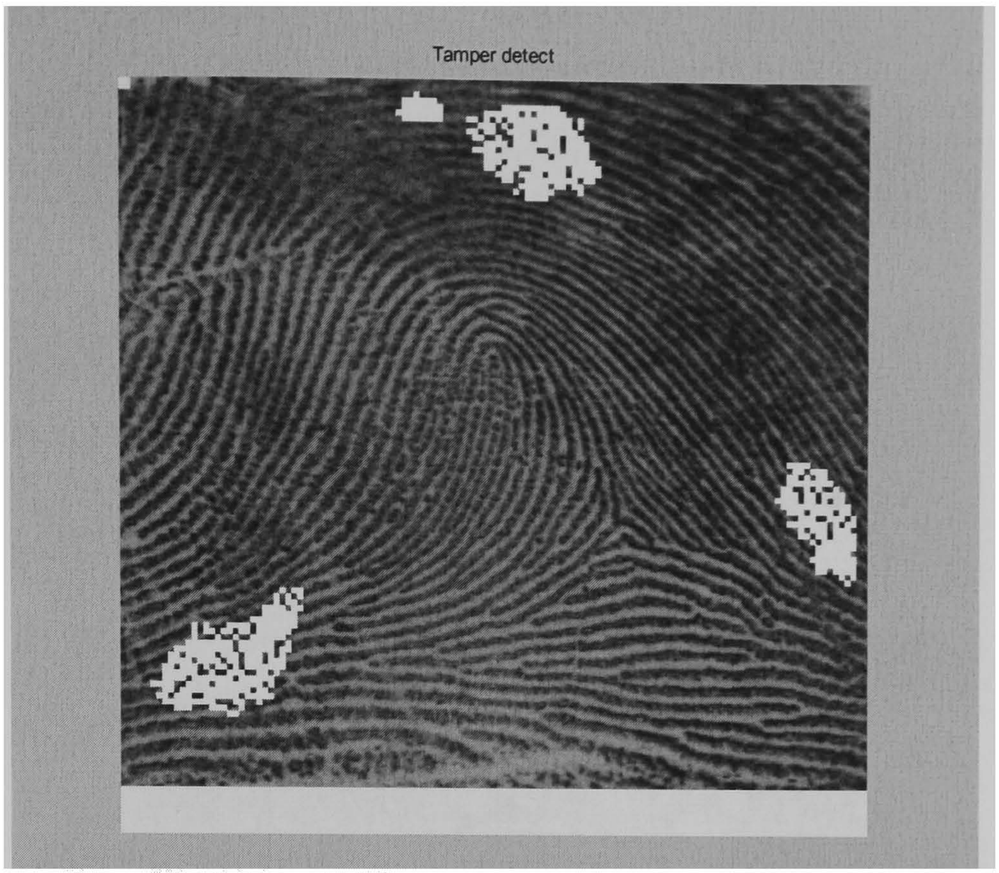


Figure 5.25. Level 1 detection- fingerprint1

Fingerprint1 was manipulated using healing brush tool and cloning tool. The manipulated sizes are ~60 x 50 and ~100 x 100 pixels.

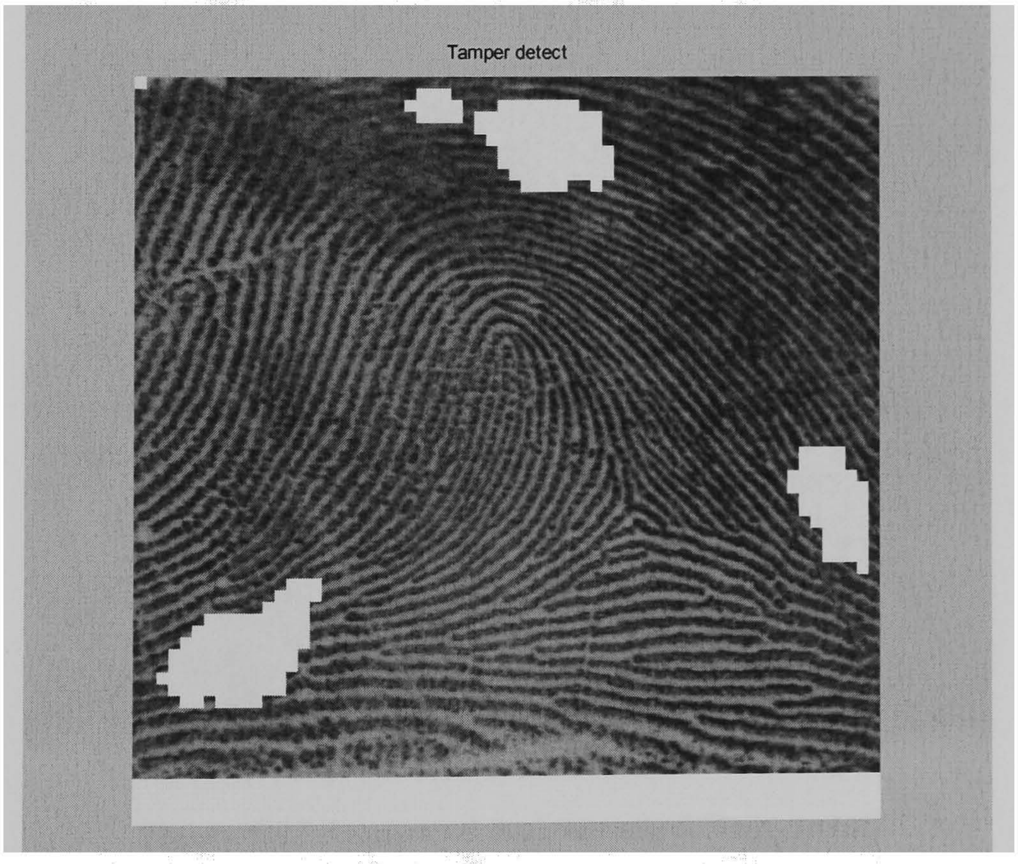


Figure 5.26. Level 2 detection- fingerprint1

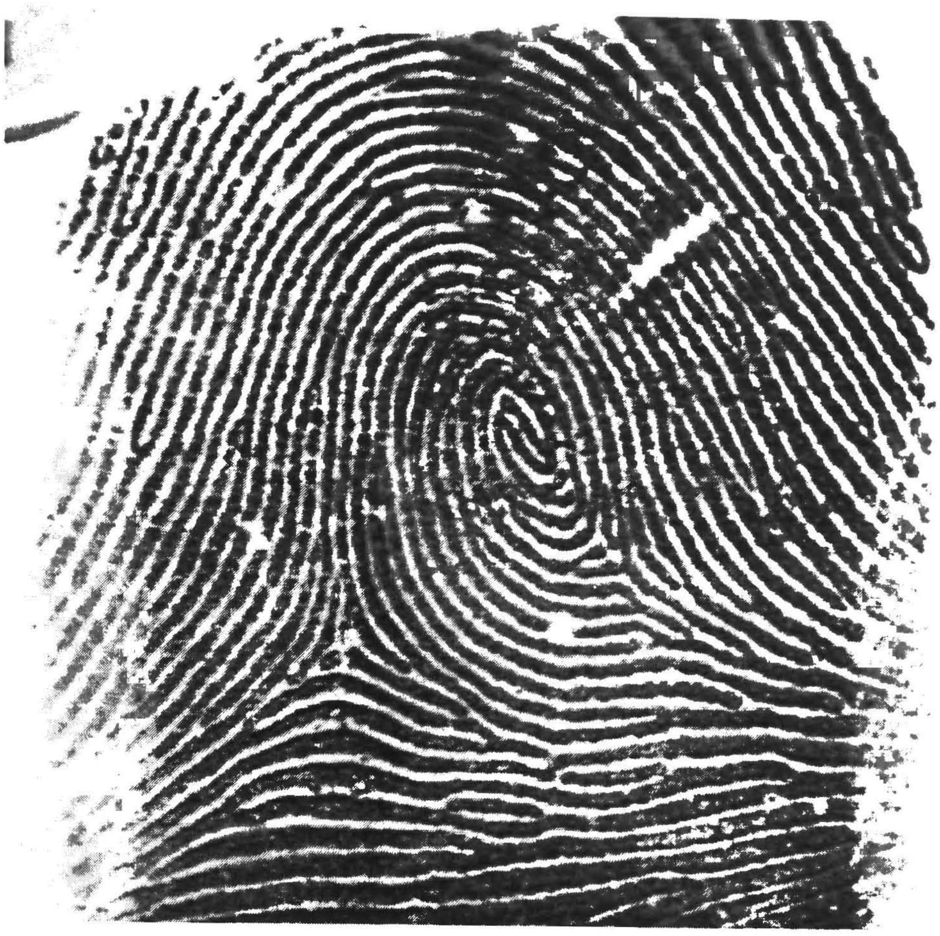


Figure 5.27. Watermarked fingerprint2 PSNR = 54.9982 dB

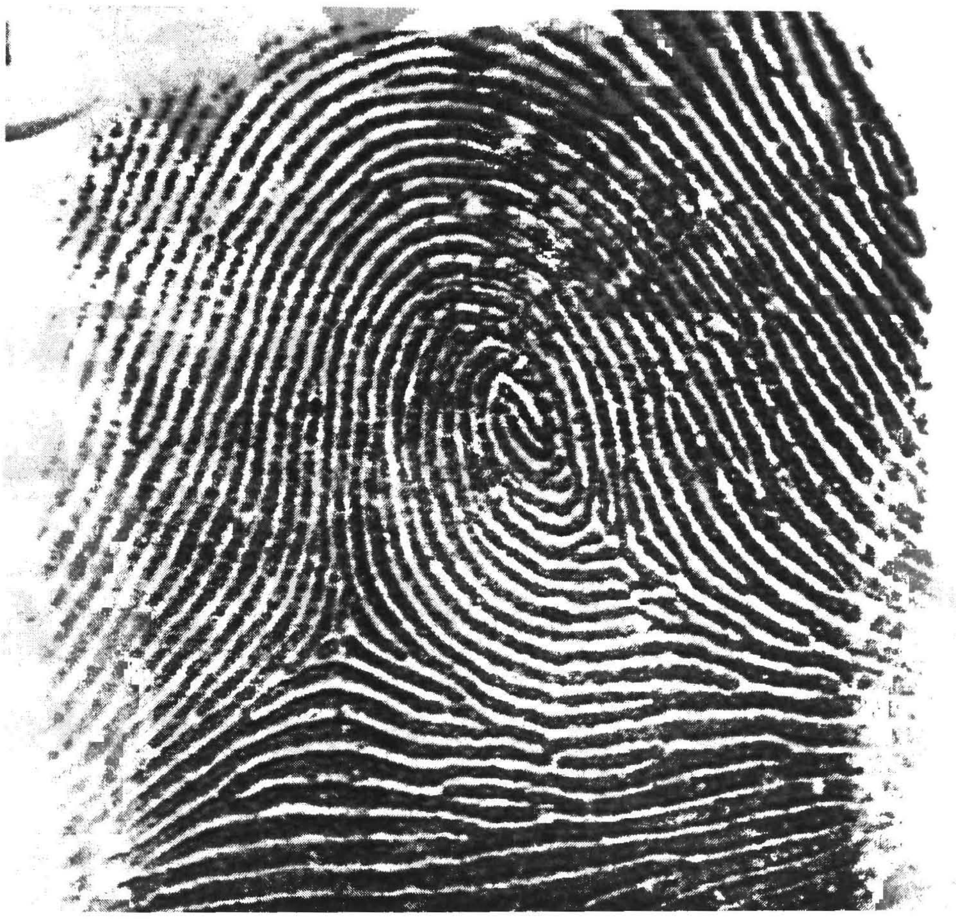


Figure 5.28 Tampered watermarked fingerprint2

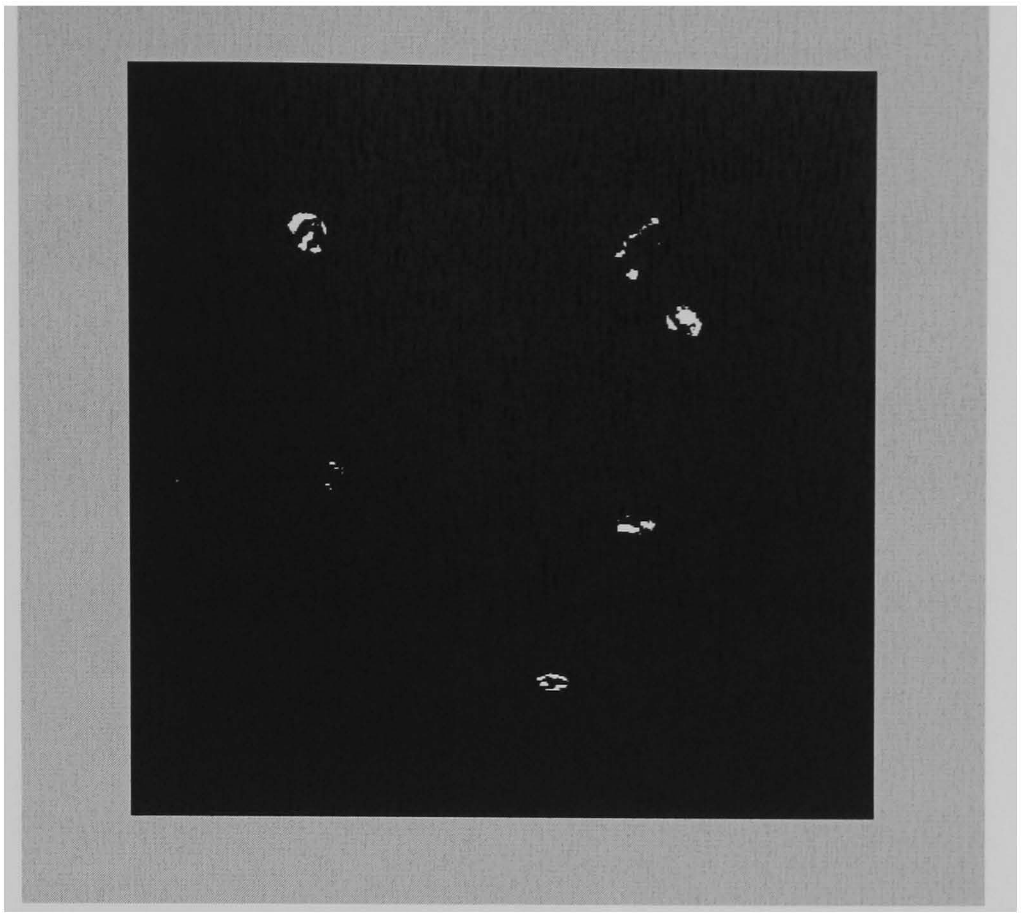


Figure 5.29. Image Difference

Fingerprint2 was manipulated using cut and paste and cloning tool. This time the manipulation size is smaller ranging from ~ 10 x10 to 40 x 100 pixels.

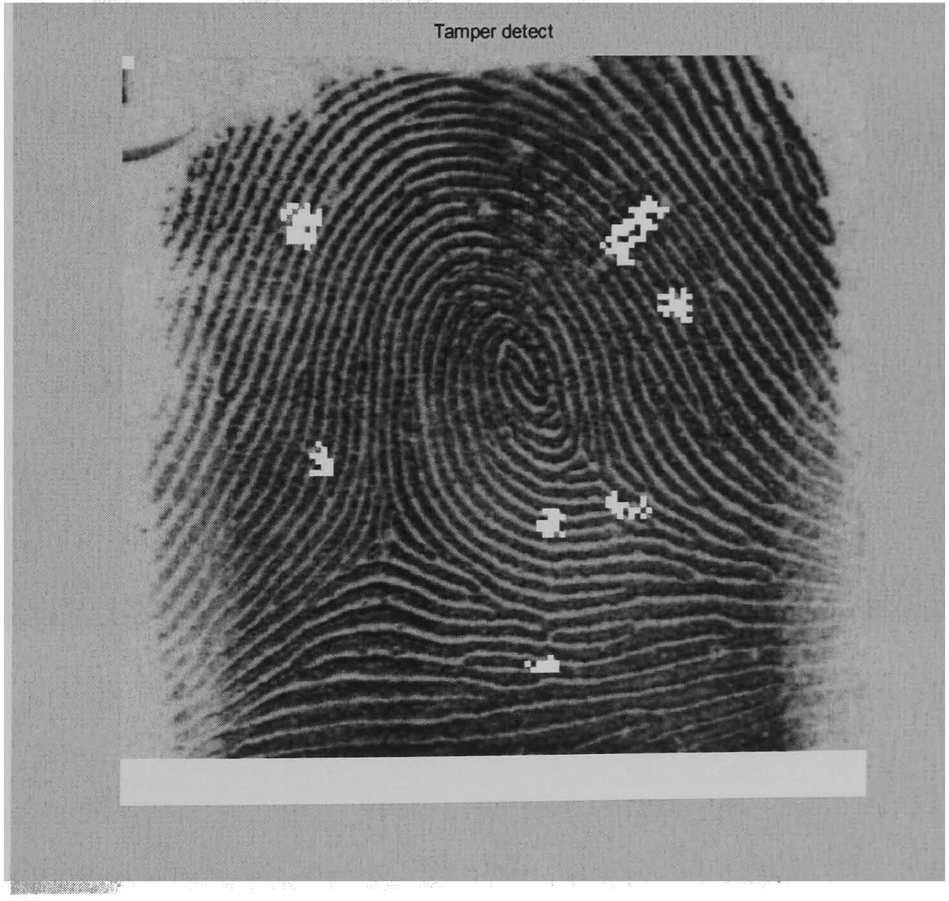


Figure 5.30. Level 1 detection – fingerprint2

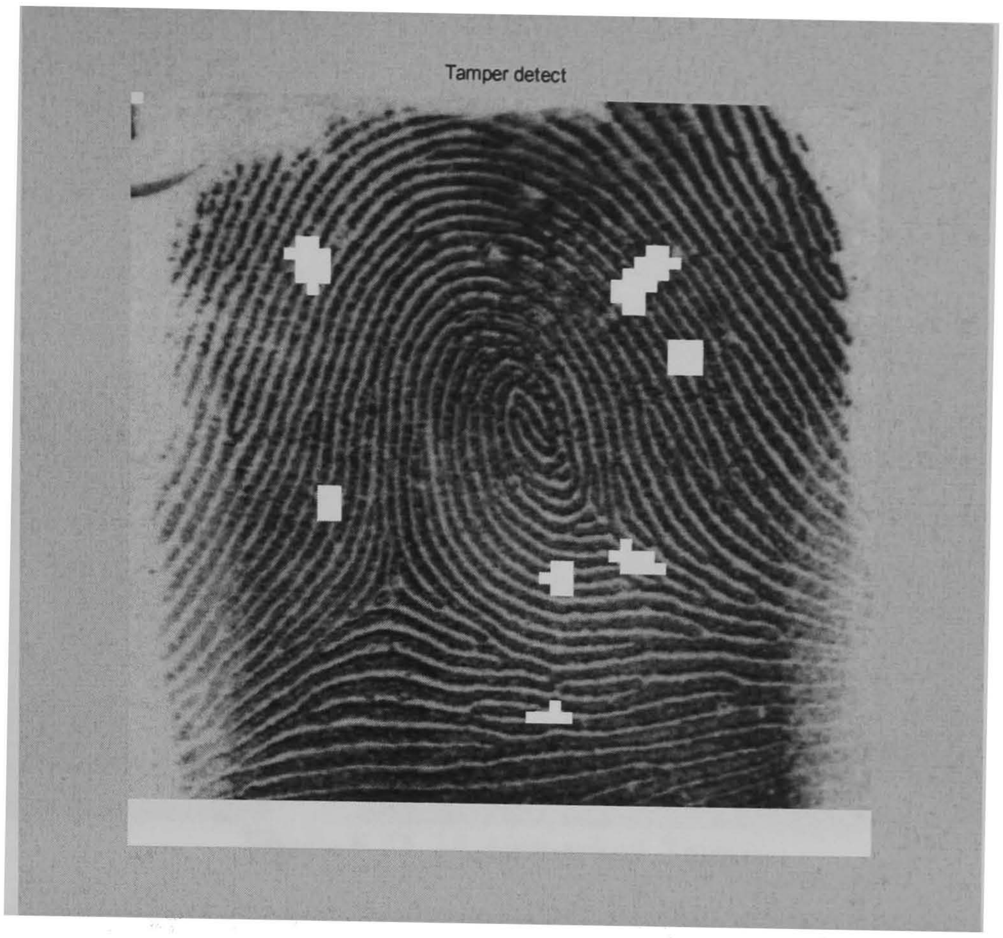


Figure 5.31. Level 2 detection – fingerprint2

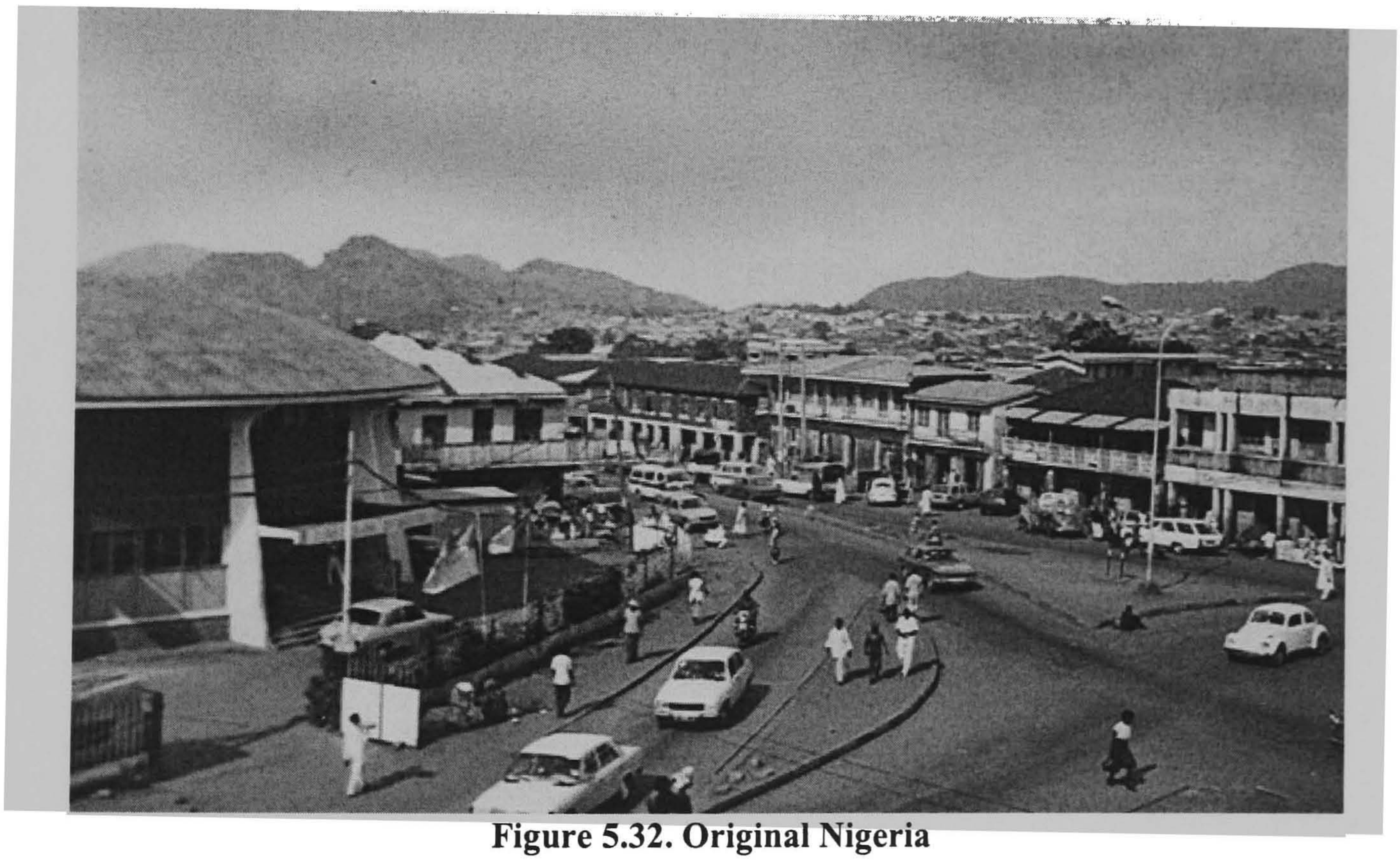


Figure 5.32. Original Nigeria

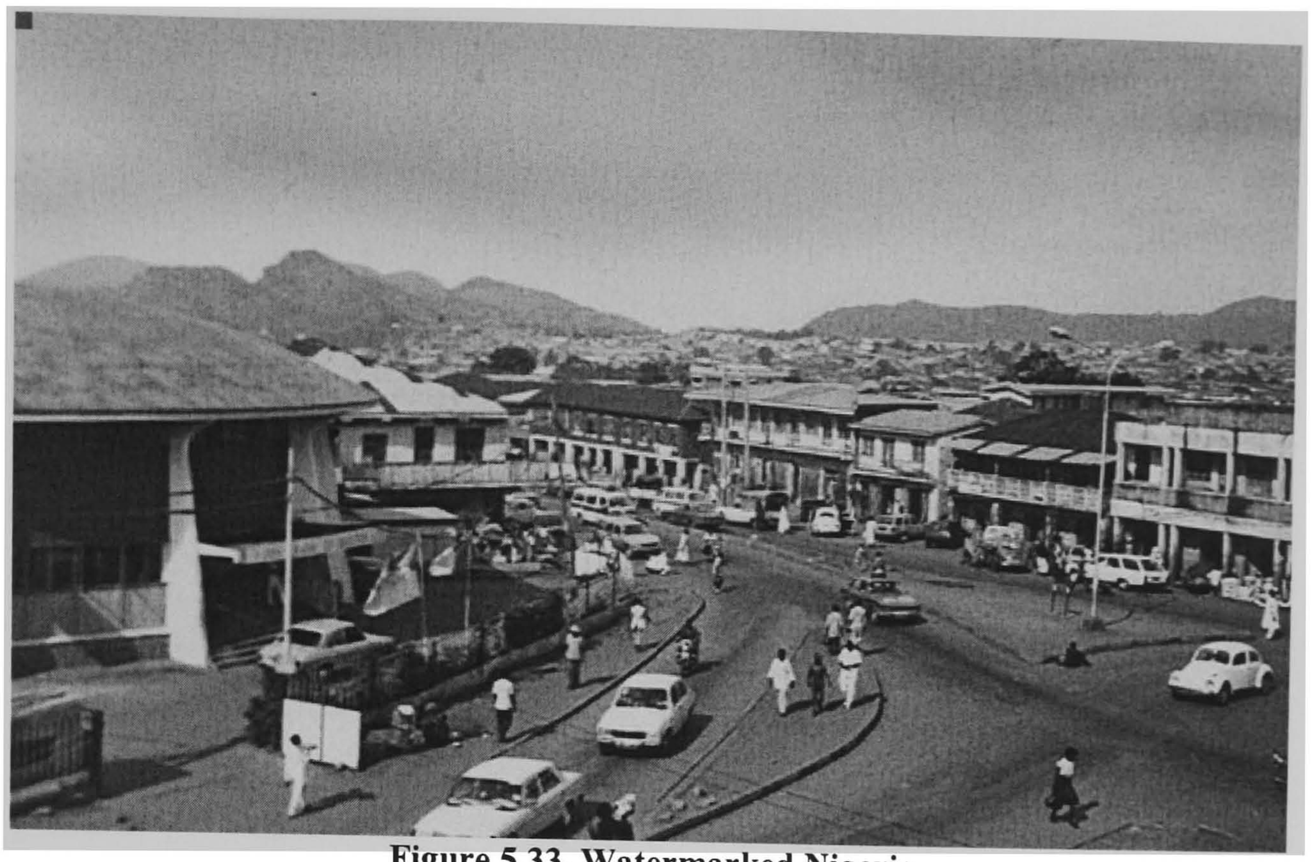


Figure 5.33. Watermarked Nigeria

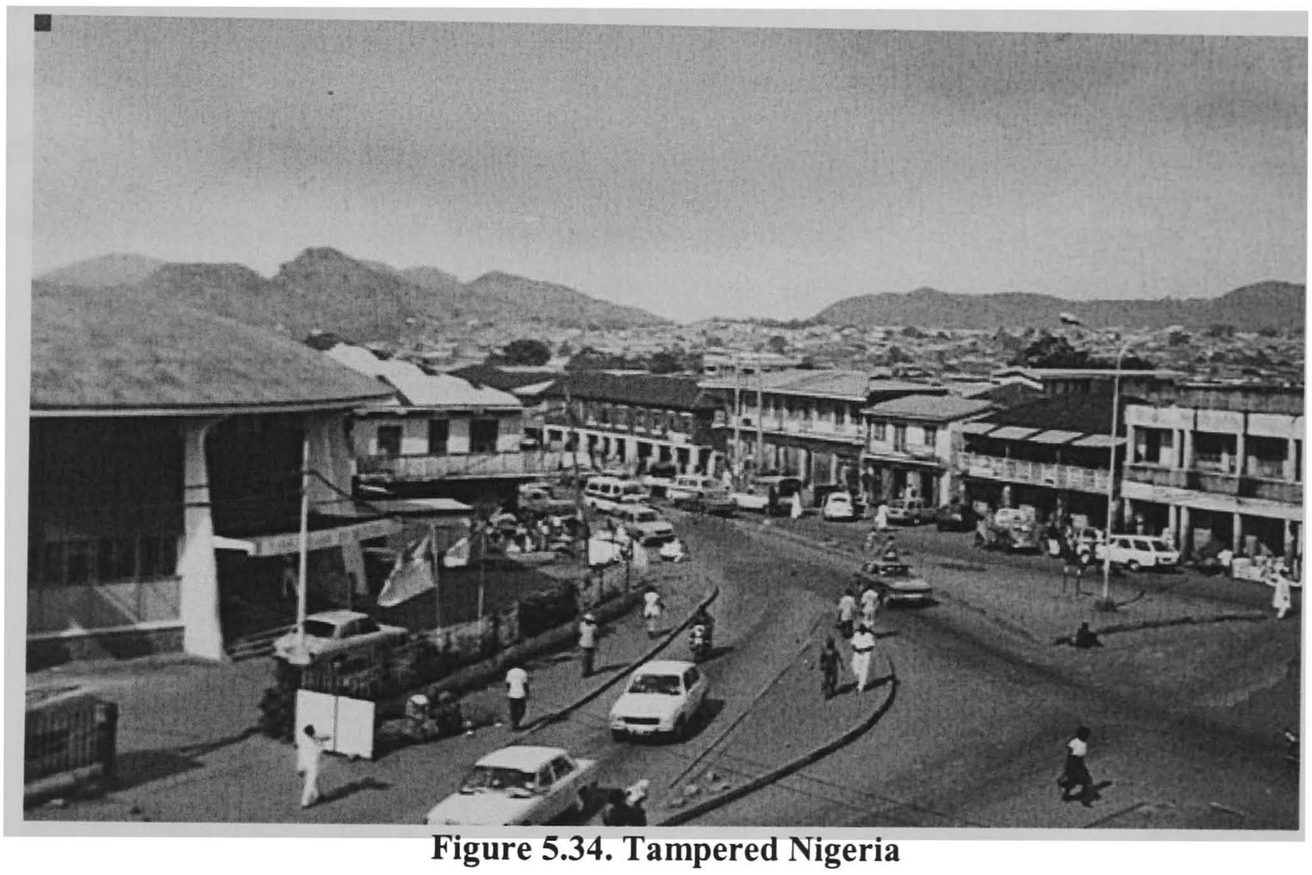


Figure 5.34. Tampered Nigeria

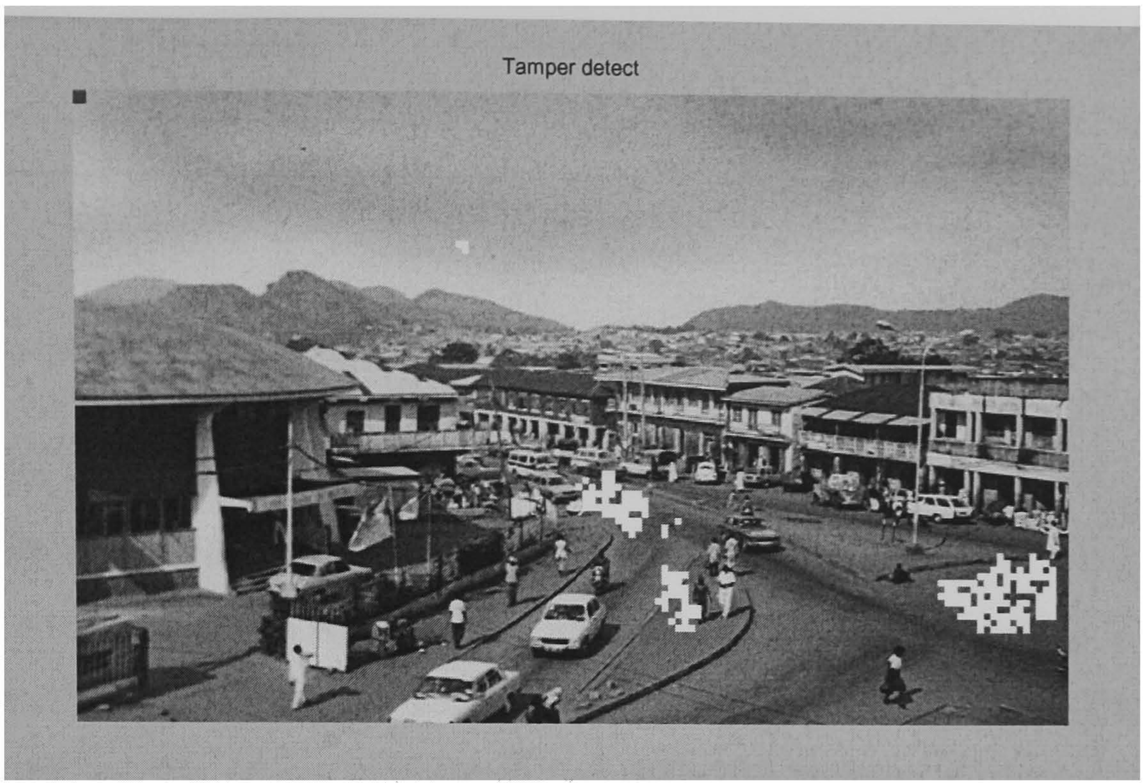


Figure 5.35. Level 1 detection- Nigeria

Nigeria was manipulated by removing some objects from the image. Four people were removed including one person and his shadow at the centre. A Volkswagen at the bottom right corner was also removed. A small area in the sky was also manipulated. Paintbrush, healing brush and cloning tools were used.

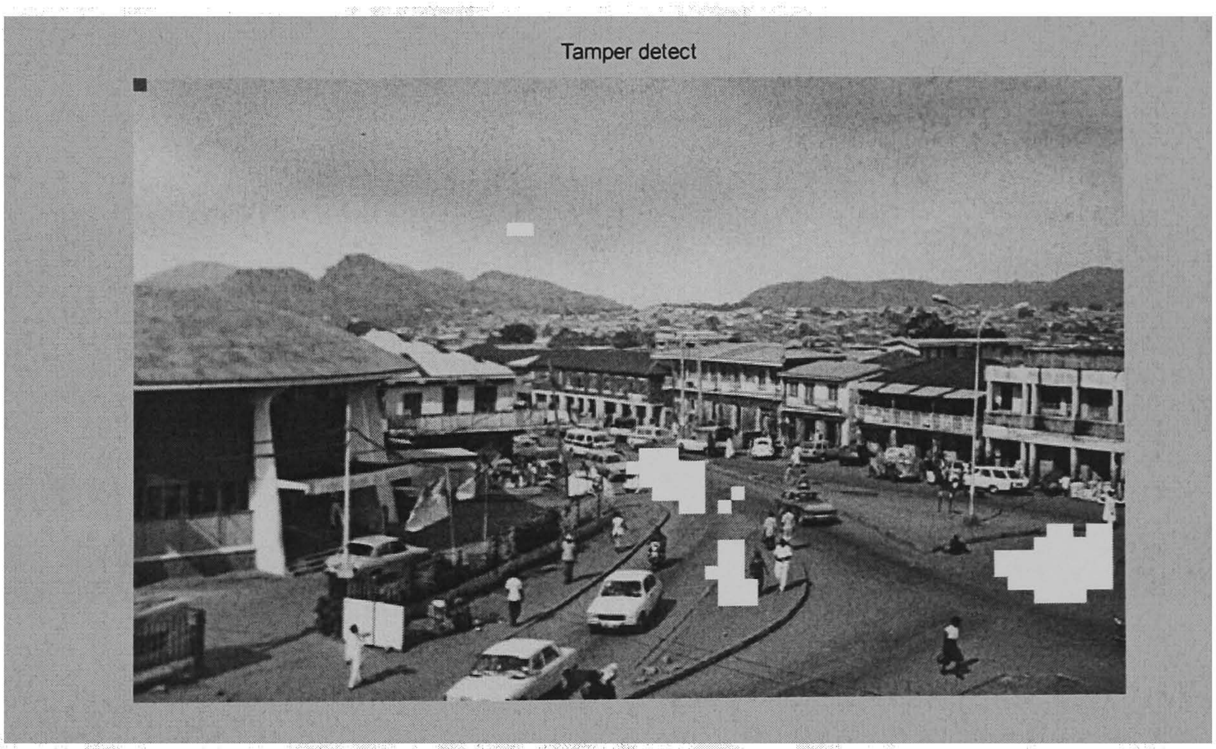


Figure 5.36. Level 2 detection - Nigeria

Table 5.2 shows the missing detection rate using level-1 and level-2 detection. For level-1 detection, we have a maximum of 16% of missing detection rate. We achieved at least 99.9% detection rate for level-2 detection.

	Ultrasound (800x600)	Fingerprint1 (512x512)	Fingerprint2 (512x512)	Nigeria (600x376)
Level1	10%	15%	13%	16%
Level2	0.1%	0.06%	0.02%	0.03%

Table 5.2. Miss detection rate

- Recovery in the middle region

We carried out another experiment to test the performance of our recovery algorithm to test when the tamper is made near to the centre of the image. For ultrasound images, this is highly likely because the region of interest happens to be in the centre of the image. We tampered with a watermarked image (k=3739) with tampering size of 20x20 pixels (figure 5.37) and 100x100 pixels (figure 5.39). For the 20x20 tamper, one block situated at the middle is not recovered. For 100x100 tamper, seven blocks were not recovered including the block in the middle of the image. The analysis of this will be discussed in chapter 6.

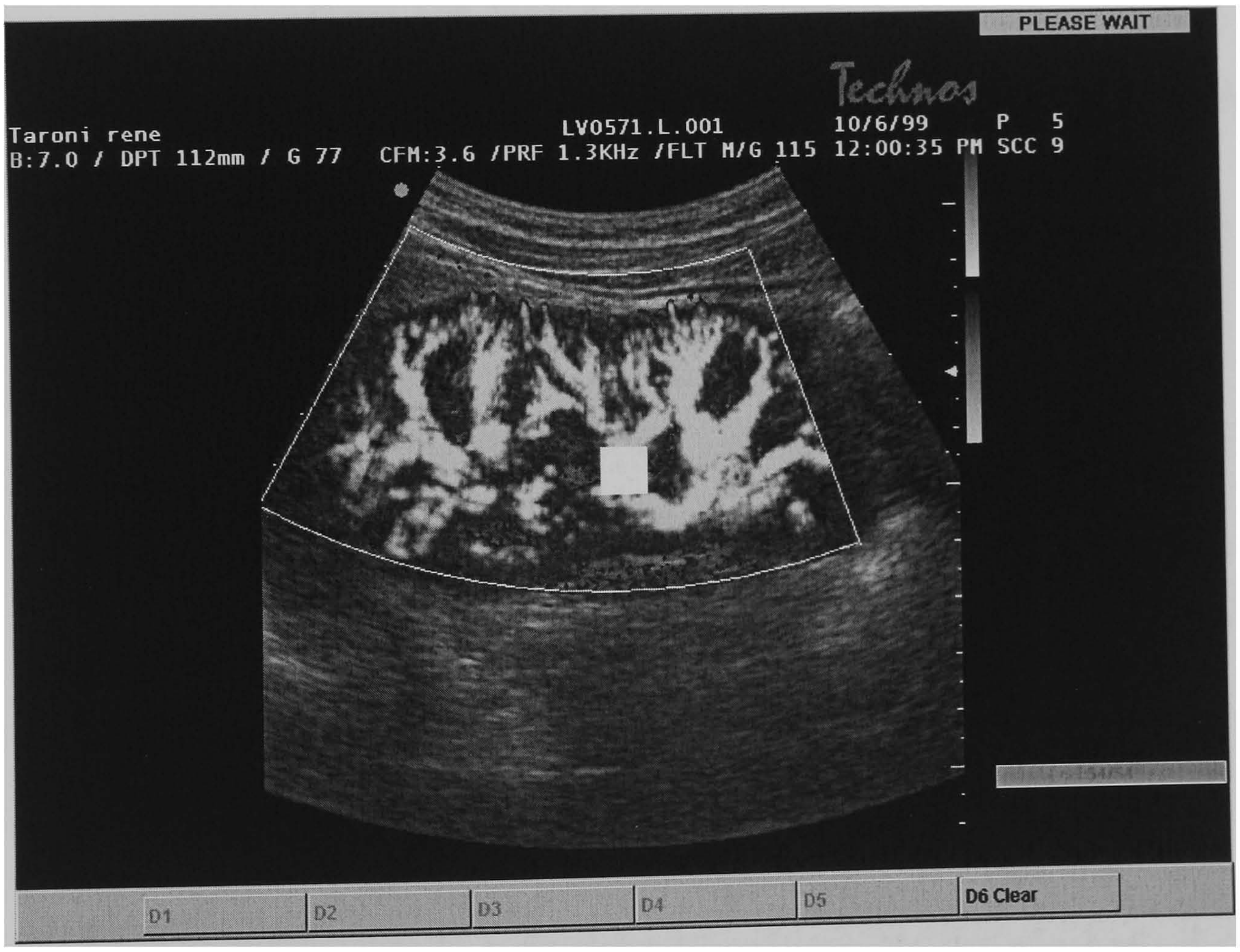


Figure 5.37. Tamper in the middle 20 x 20 pixel

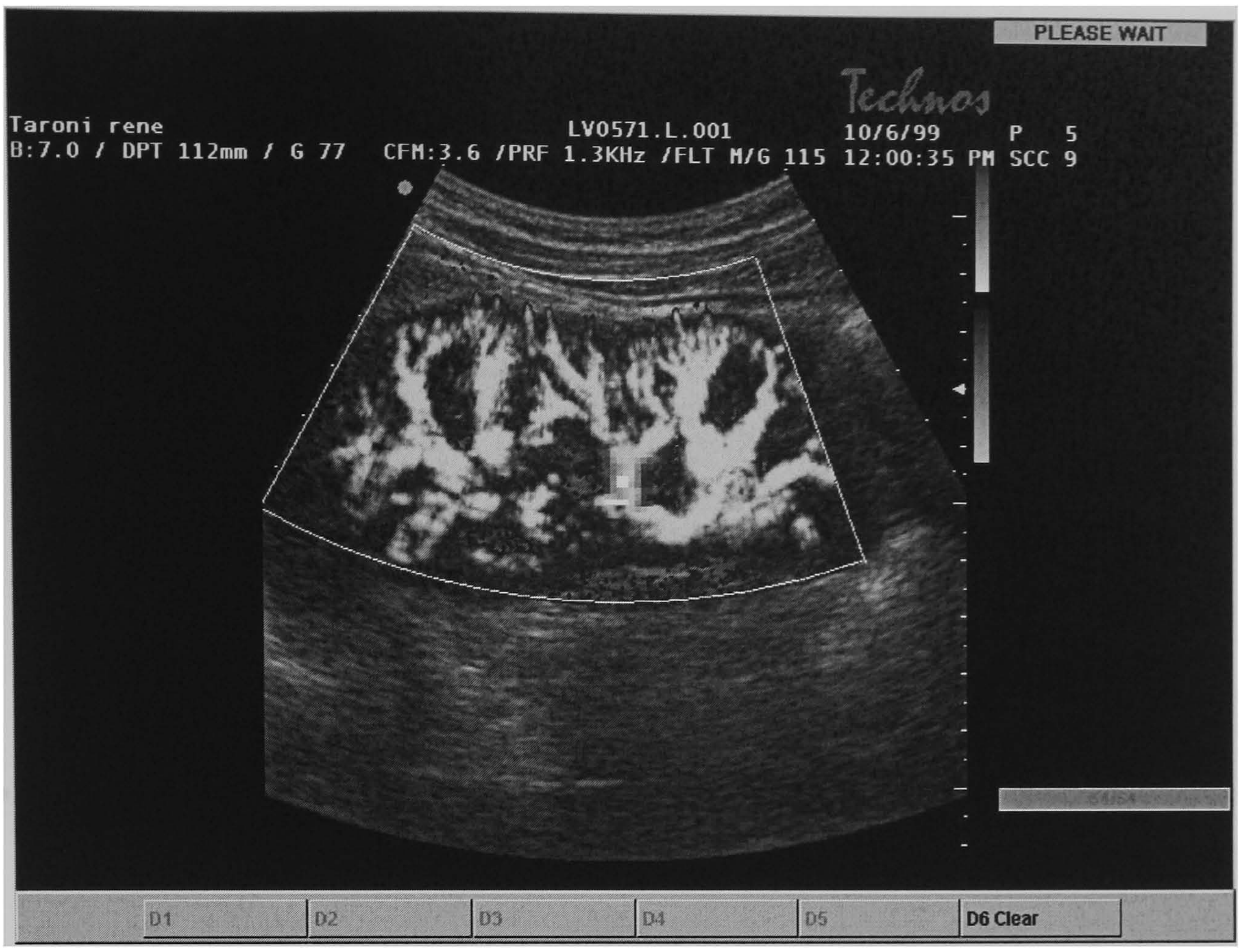


Figure 5.38. Recovered image of figure 5.37

Figure 5.38 shows that the block in the middle is not recovered, while the blocks around it have been recovered.

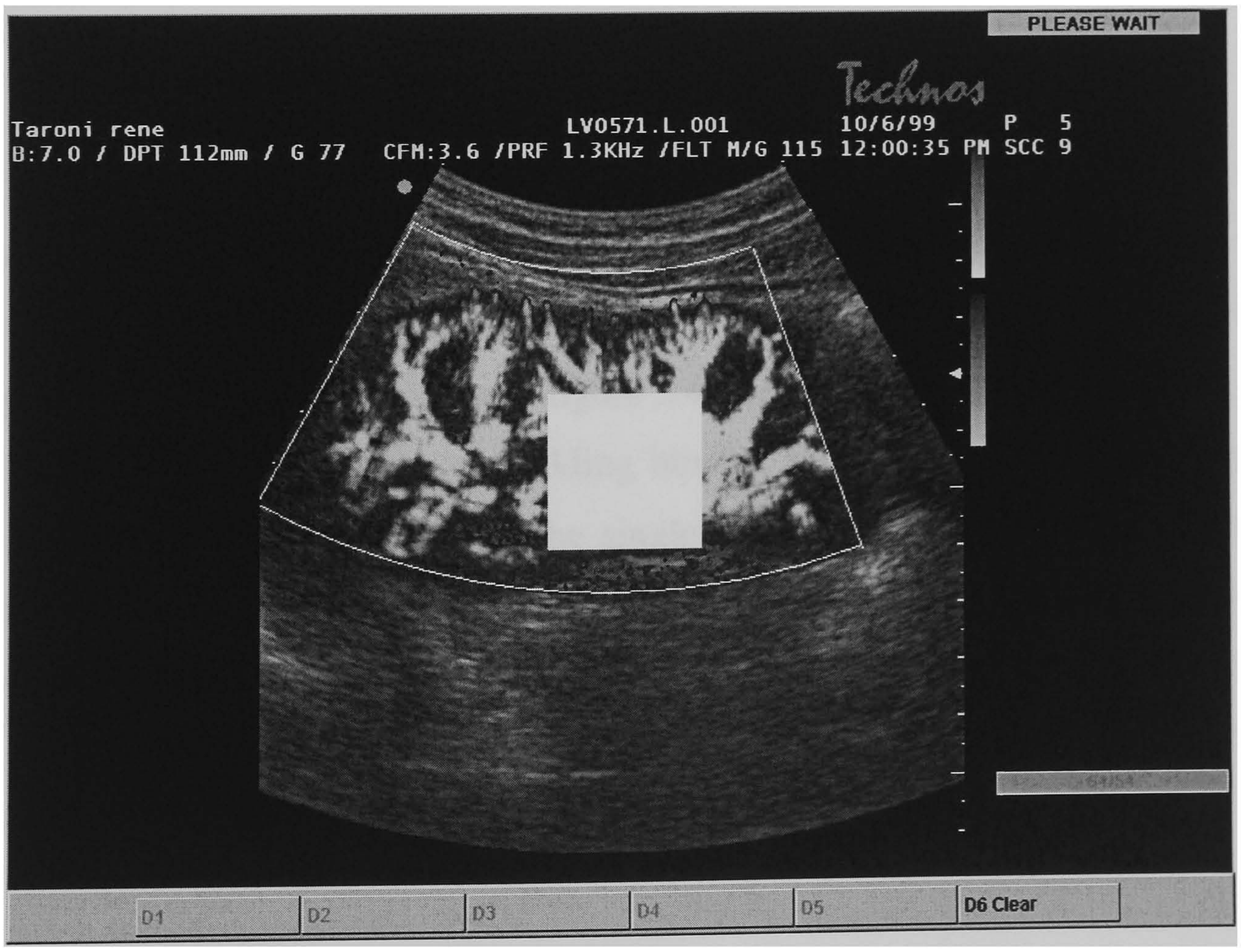


Figure 5.39. Tamper in the middle 100 x 100

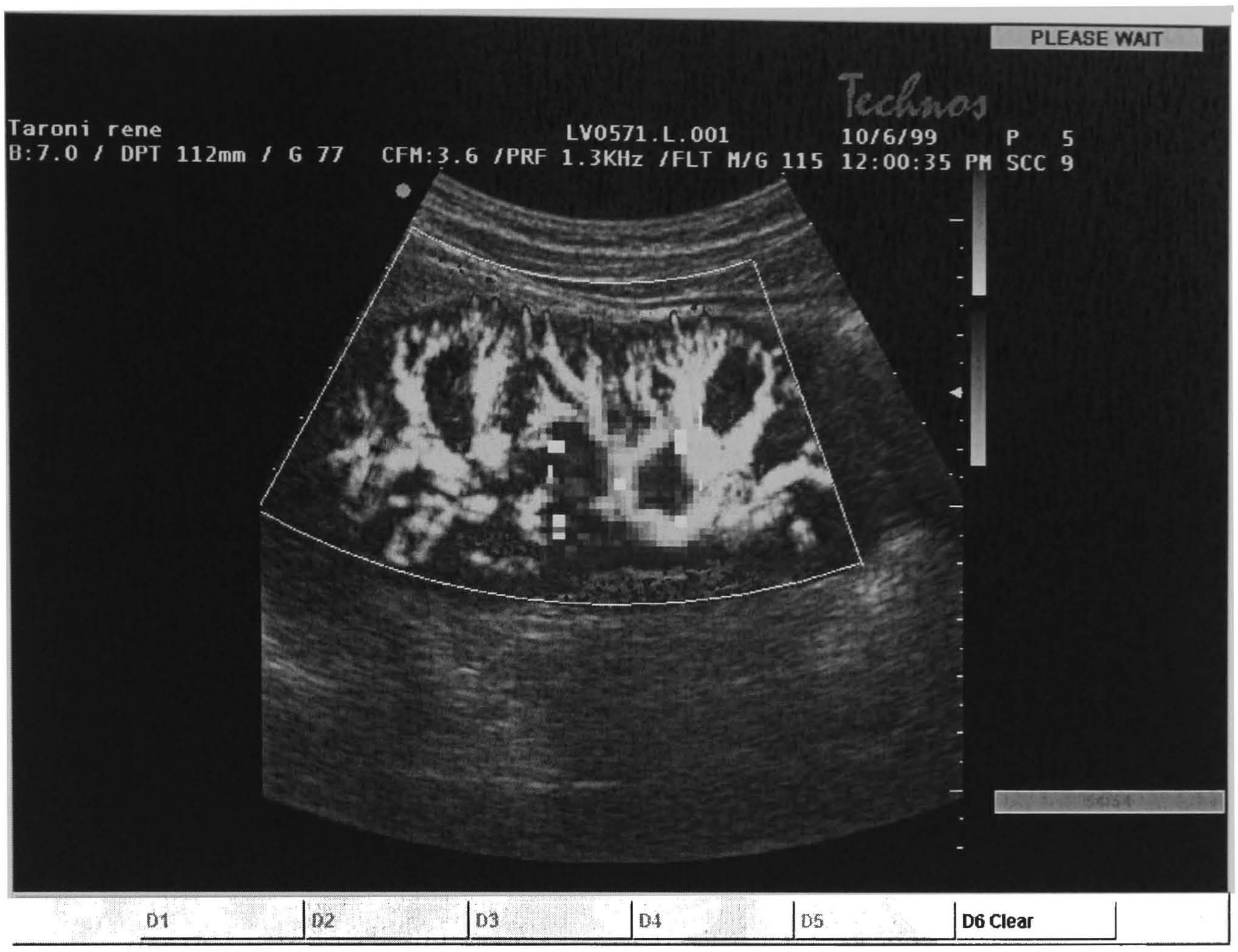


Figure 5.40. Recovered image of figure 5.39

Figure 5.40 maintains that the block in the middle cannot be recovered by our method. In addition, some blocks at the vertical edge also cannot be recovered using our method.

- Recovery rate

An experiment to see the distribution of tampering, the size of the tampering effect and the rate of recovery was also carried out. We tampered with the watermarked (k=3739) image using spread-tampered blocks and single tampered blocks with a tampered area ranging from 10% to 50% as shown in figure 5.41 and figure 5.42. The spread-tampered blocks are the same size as the embedding blocks. Figure 5.43 shows the number of blocks that were not recovered from the single tampered block. We also changed the direction column-wise to see the effect. For a 10% column-wise single tampered block, we have a 100% recovery as in figure 5.44. This shows that the distance for those blocks and the mapped blocks were more than 1/10 of the image size. The results will be discussed further in chapter 6.

Figure 5.44 shows the number of un-recovered blocks for a single-tampered chunk. We obtained a 100% recovery for spread tampered blocks. The analysis will be discussed in chapter 6. Please see Appendix C for the recovered images.

5.5.6 Conclusion

We proposed a watermarking scheme that can detect and localise tampered and recovered images. The purpose is to verify the integrity and authenticity of medical images. We presented our watermarking procedures that include data embedding, tamper detection and recovery procedure. The experimental results demonstrate that the precision of tamper detection and localisation is close to 100% after level-2 detection. The tamper recovery rate is better than 86% for a less than half a tampered image.

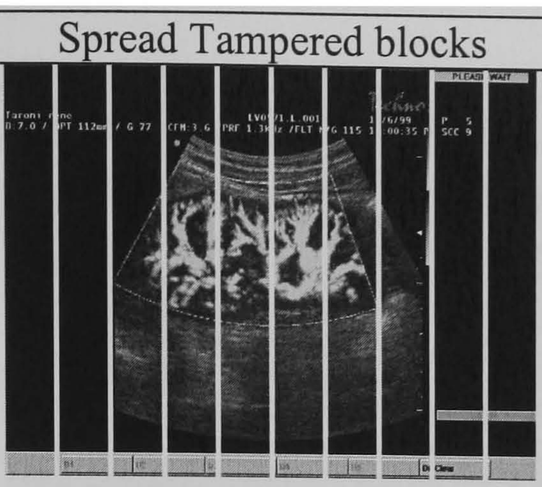
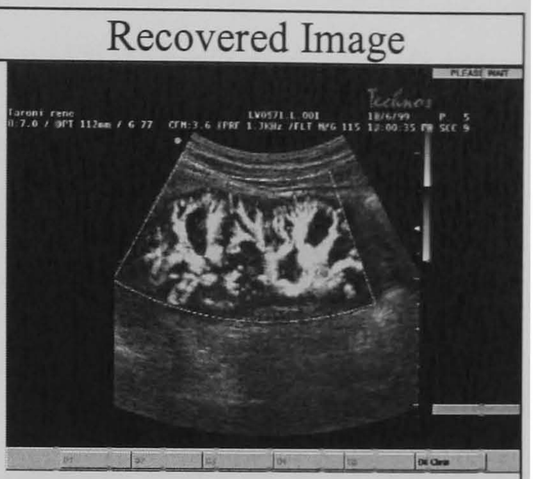
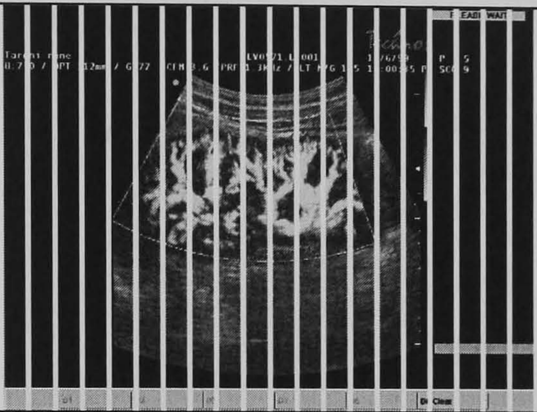
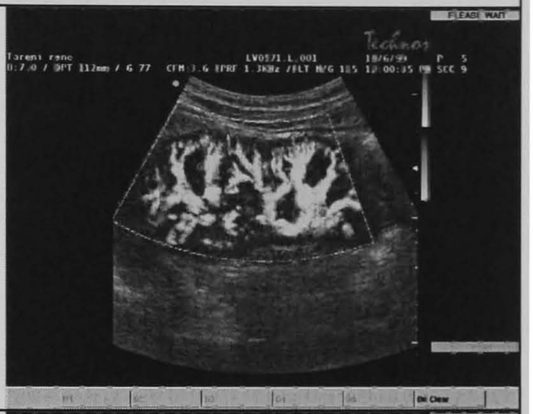
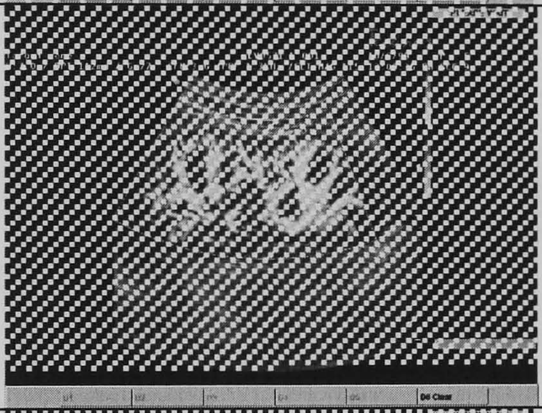
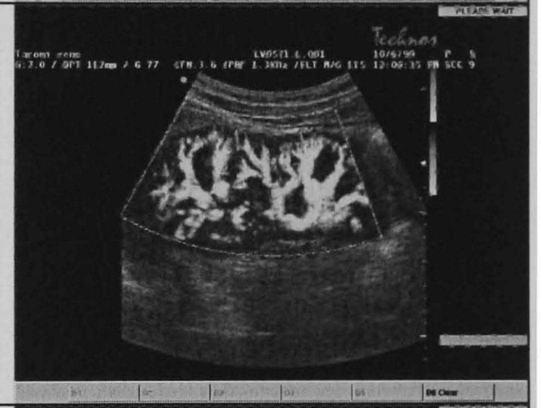
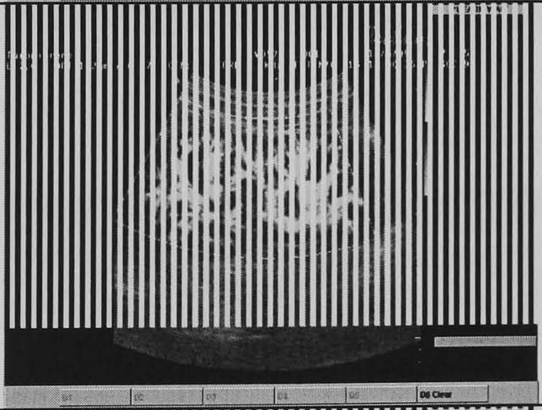
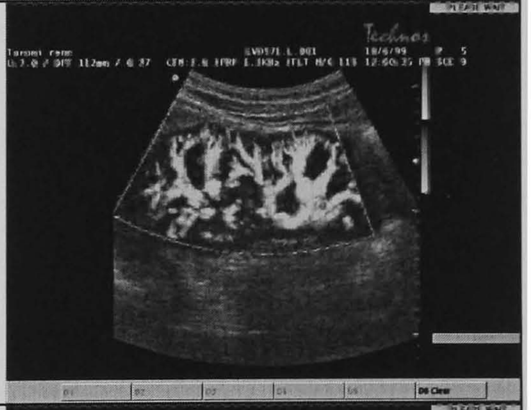
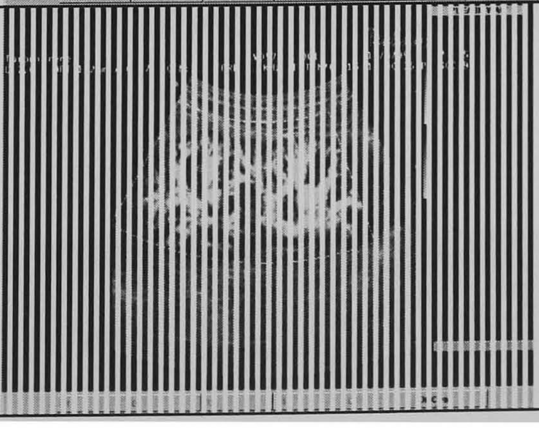
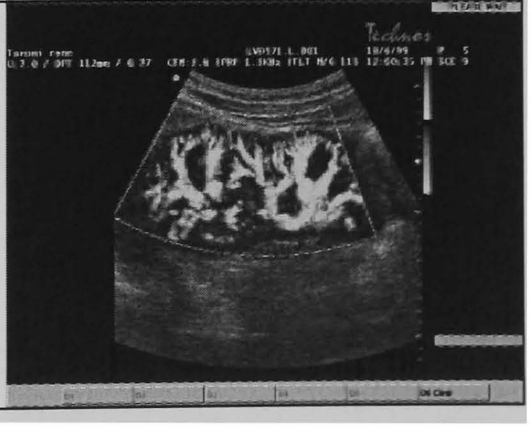
Tampering rate	Spread Tampered blocks	Recovered Image
10%		
20%		
30%		
40%		
50%		

Figure 5.41. Spread Tamper and recovered images

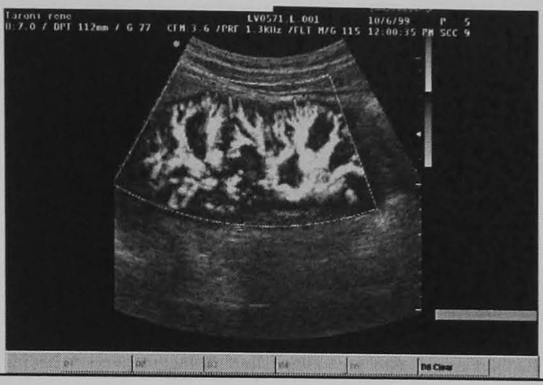
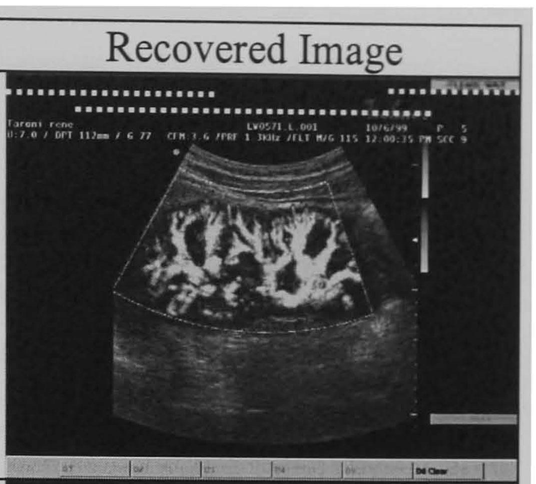
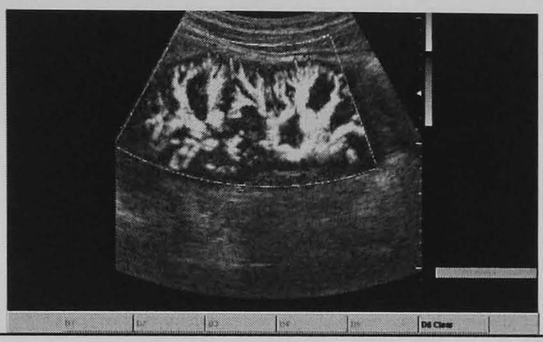
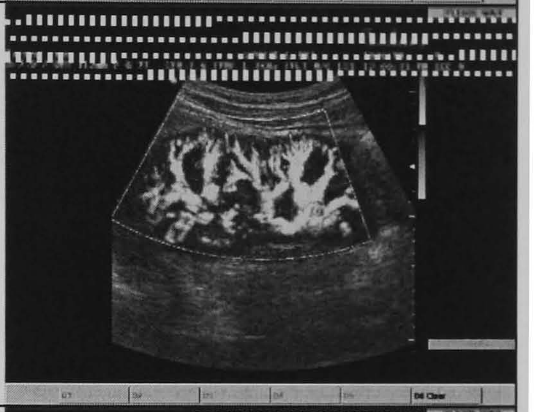
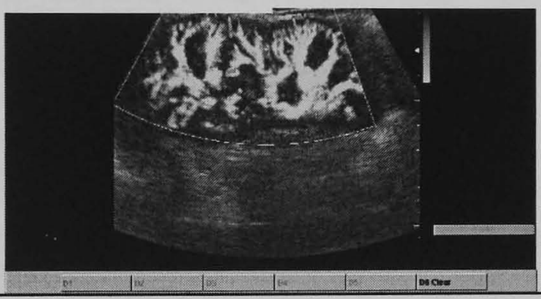
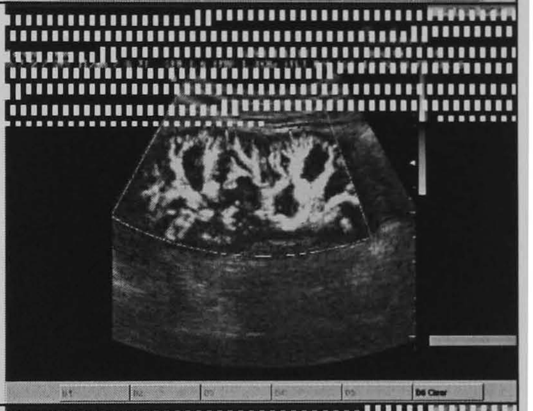
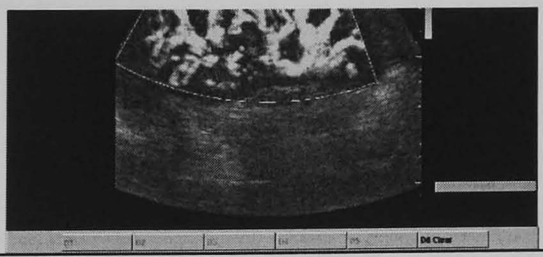
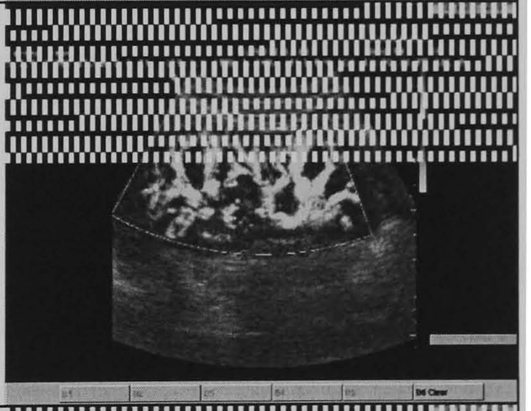
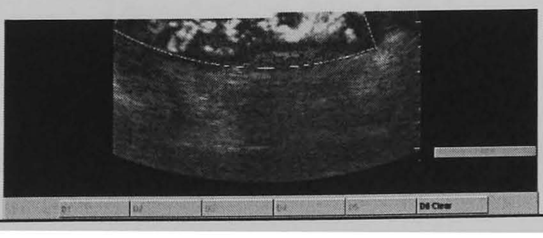
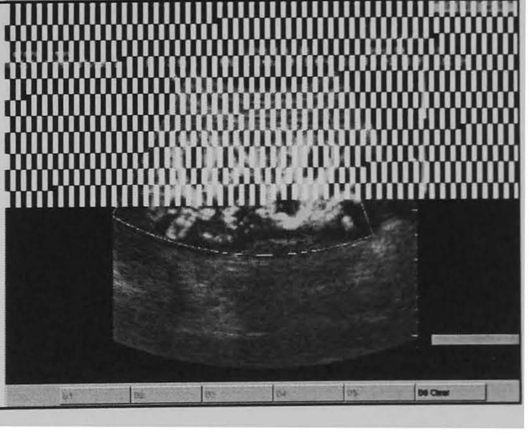
Tampering rate	Single tampered block	Recovered Image
10%		
20%		
30%		
40%		
50%		

Figure 5.42. Block tamper and recovered images

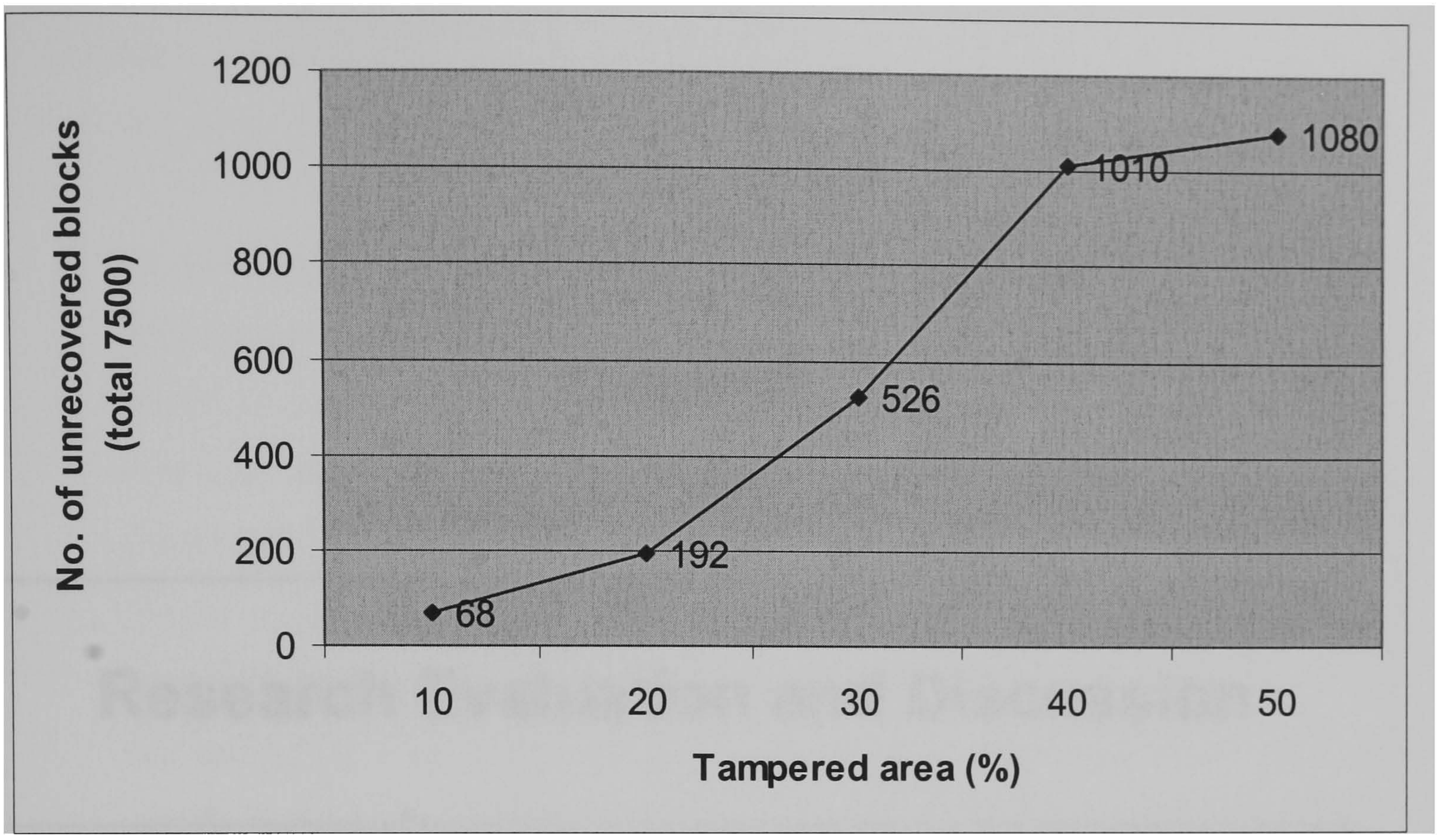


Figure.5.43. The number of un-recovered blocks for single tampered blocks

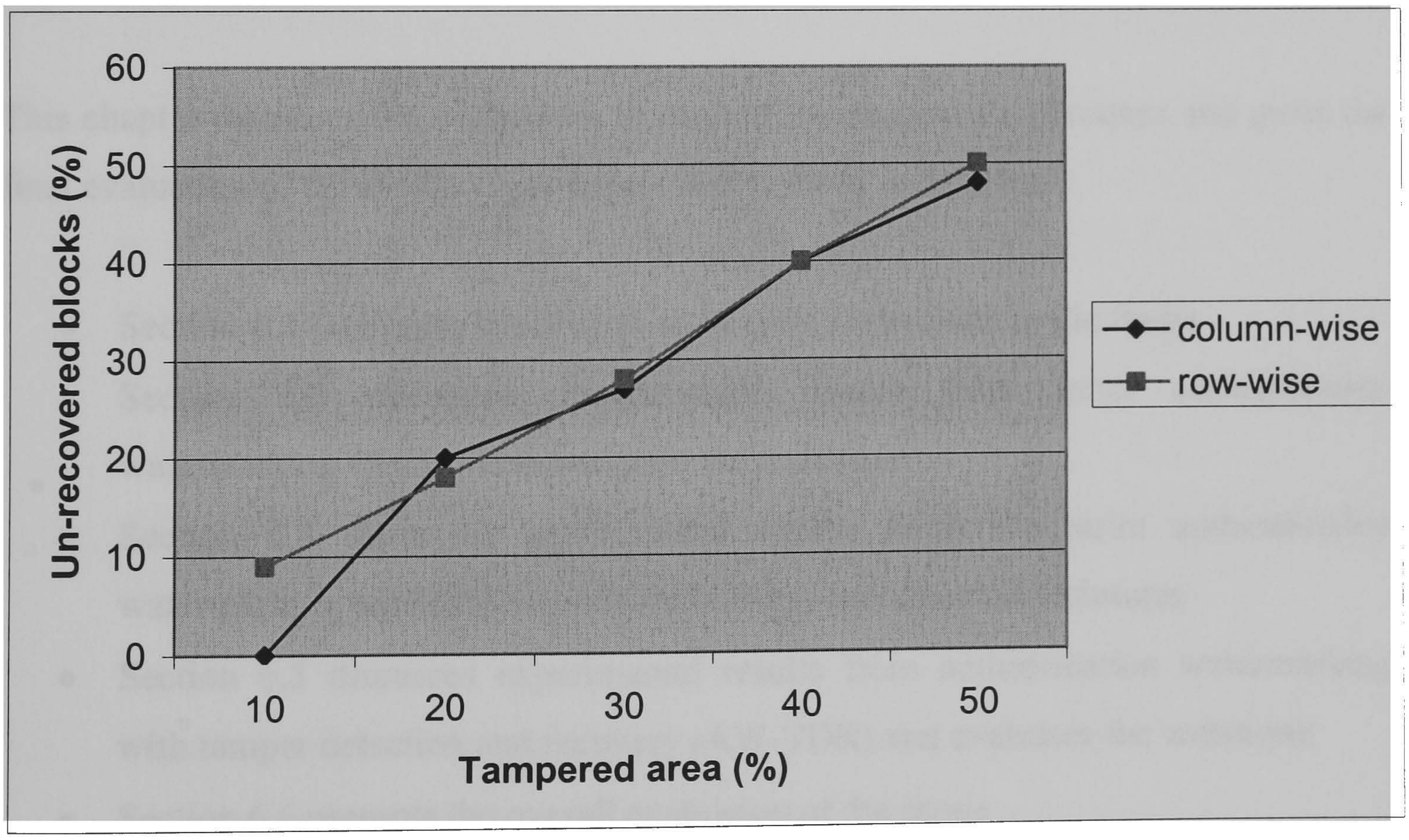


Figure 5.44. Percentage of un-recovered blocks for column and row- wise tampered

Chapter 6

Research Evaluation and Discussion

6.1 Introduction

This chapter discusses the evaluation of each of the proposed techniques and gives the final evaluation of the thesis. This chapter is structured as follows:

- Section 6.2 highlights the criteria to be used for evaluating the thesis
- Section 6.3 discusses experimental results from strict authentication watermarking (SAW) and evaluates the technique
- Section 6.4 discusses experimental results from the strict authentication watermarking with JPEG (SAW-JPEG) and evaluates the technique
- Section 6.5 discusses experimental results from authentication watermarking with tamper detection and recovery (AW-TDR) and evaluates the technique
- Section 6.6 presents the overall evaluation of the thesis

6.2 Evaluation Criteria

We evaluate our watermarking system according to the requirements outlined by Tong Liu, Zheng-ding Qiu (2002) and Lin, Chang (2000):

- Invisibility: The embedded watermark is invisible. It is the basic requirement of keeping the quality of marked images. The marked image must be perceptually identical to the original one under normal observation. It is a question of making sure that the visual impact of watermarking is as weak as possible so that the watermarked image remains identical to the originals.
- Detect tampering: An authentication watermarking system should detect any tampering in a marked image. This is the most fundamental property to reliably test the authenticity of the image. The system must be sensitive to malicious manipulations such as altering the image in specific areas.
- Security: The embedded watermark cannot be forged or manipulated. In such systems, the marking key is private and should be difficult to deduce from the detection of information. Insertion of a mark by unauthorised parties should be difficult.
- Identification of manipulated area or localization: The authentication watermark should be able to detect the location of altered areas, and verify other areas as authentic. The detector should also be able to estimate what kind of modification had occurred.
- Reconstruction of altered regions: The system may need the ability to restore, even partially, altered or destroyed regions in order to allow the user to know what the original content was of the manipulated areas.

6.3 Strict Authentication Watermarking (SAW)

- Invisibility and image quality

Invisibility is achieved as the maximum difference to the original image is only by one grey level. Figure 6.1 indicates how much visual difference for each grey level.

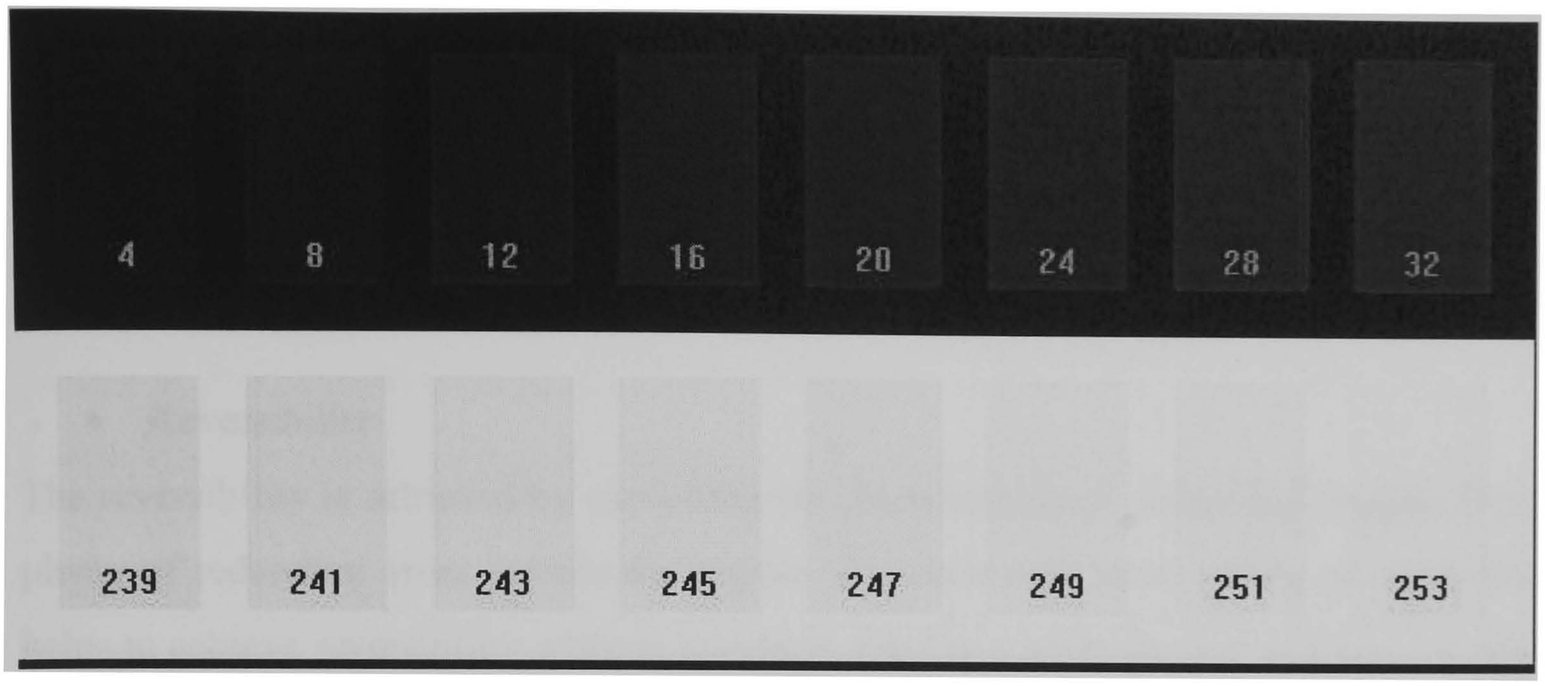


Figure 6.1. Grey levels

With only 256 bits embedded, distortion is very low with PSNR at 2.6 x 10^6 dB. However, the objective of any medical image would lie in a specific region of interest. Although as non-medics we do not know where the exact area of interest is for an ultrasound image, it is apparent that the region of interest only lies where the object projected by the ultra sound lies. We have made sure that the areas concerned are not included for embedding purpose. If the way the ultrasound image is taken and stored is changed then the technique will not be relevant anymore.

- Security

The security for this technique depends on the security of the key used. Bigger key space will increase security, but will result in difficulty to manage them. As Tong and Zheng-ding (2002) stressed, any algorithm alone cannot guarantee the security of the system. It is necessary to define a set of scenarios and specifications describing the operation and rules of the system, such as management of the keys or the communication protocols between consultants, doctors, technicians and so forth.

- Tamper detection

The technique will detect tamper by comparing the signature produced by hashing the region of interest. Any changes inside the area will have a significant change in the signature produced by the hash function. The system however will not detect changes made outside the region of interest. If this is of concern, then the system can be made to produce a signature of the whole image, which is embedded in the region of non-interest. At the receiver's side the watermark, which is the signature, is extracted, and reverts the values to the original state. The signature is then calculated and compared to the received.

- Reversibility

The reversibility is achieved by exploiting the characteristic of ultrasound images. With plenty of redundant areas outside the region of interest with pixel values of zeros, this helps to achieve reversibility without having to employ a sophisticated technique unique from the literature.

- Capacity

The SAW embedding scheme achieves a high capacity for watermarks to be embedded. Table 4.3 shows that 510,000 bits could be embedded in an 800x600x8 image with distortion less than 32 dB. This gives an embedding rate of 1.06 bits/pixel. This makes the scheme superior to that of Guo and Zhuang (2003) where their embedding rate is 0.0054 bits/pixel. In applications where the watermark is embedded in a RONI, potentially an even higher embedding rate could be achieved.

The time to calculate the digital signature for a large image could be a disadvantage to this method. It is very compute intensive. For example Cao et al. (2003) noted that the time required for the sending and receiving sites for processing a digital mammogram could range from 40s for the segmented image of 7 Mb to 3 min for original 36 Mb image using Sun Sparc 690MP multiprocessor machine.

- Recovery

This method, although capable of detecting single bit changes within an entire image, has no capability to determine where the tamper has occurred or restore the tampered image to its original.

6.4 Strict Authentication Watermarking with JPEG Compression (SAW-JPEG)

- Invisibility and image quality

In this technique, the same amount of information as in SAW, is embedded into the image, however the number of embedded bits is significantly higher, in this case 64 times. Invisibility is maintained as only one grey level is involved. Using only the least significant bit, which is the eighth bit, the distortion level is kept very low with PSNR at 6.1 x 10^4 dB.

- Security, tamper detection and reversibility

The security of this technique also depends on the key. The technique is reversible and has excellent tamper detection, but no capability for reconstruction. This is the same with SAW.

- Robust to JPEG

The technique is robust to compression and was tailored to JPEG. It survives compression up to a specific level for a watermark embedded in the LSB. This approach appears unique than that reported in the literature.

- Informed authentication

The SAW technique uses informed authentication, that is it calculates the digital signature using information from the original image. In order to authenticate, the received digital signature should be compared against a new digital signature calculated for the original image. In telemedicine applications, the original image may not be available and so the digital signature must be found for the received image and compared to the received digital signature. The scheme is shown in Figure 6.2.

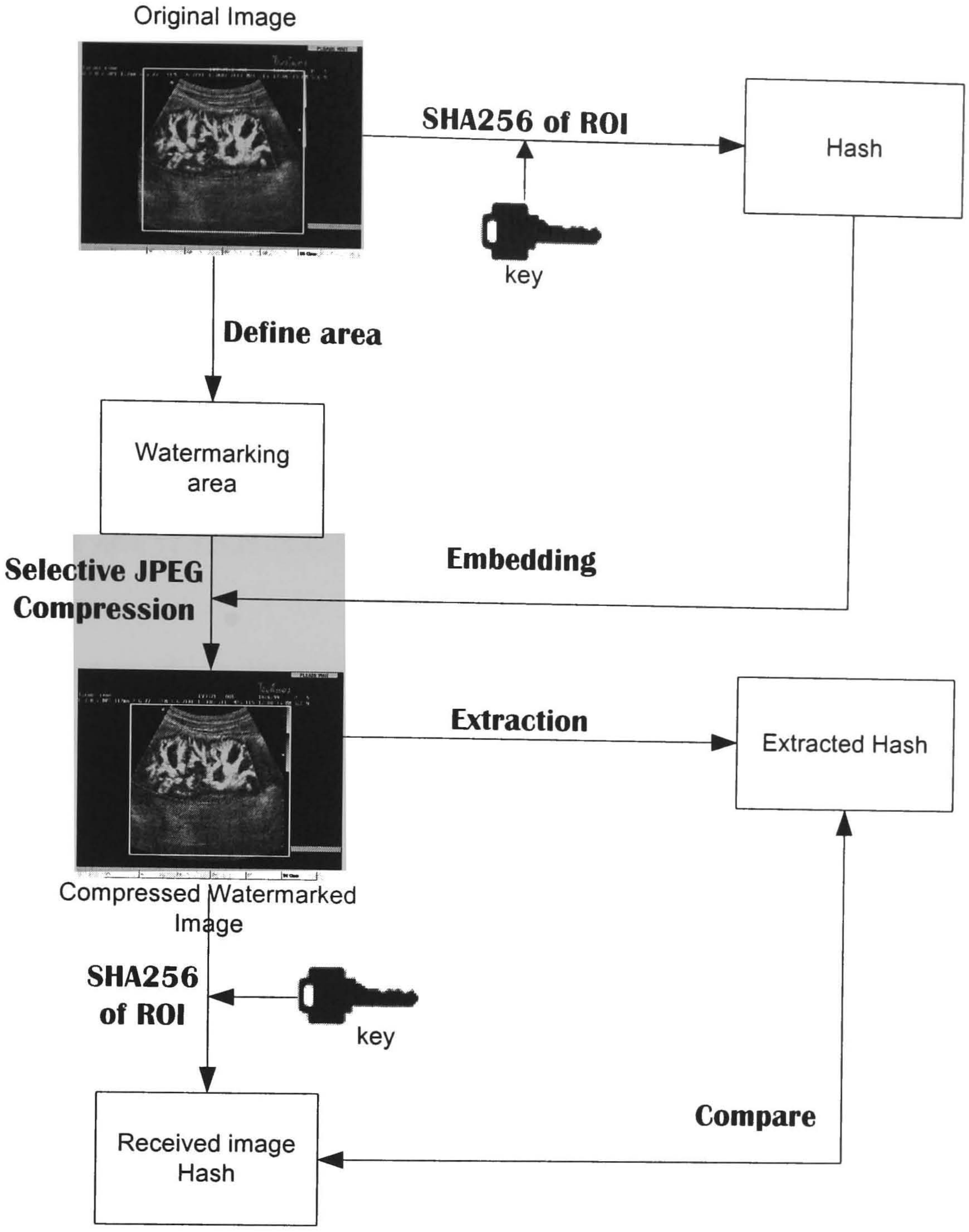


Figure 6.2 Final scheme for SAW-JPEG

6.5 Authentication Watermarking with Tamper Detection and Recovery (AW-TDR)

- Invisibility and image quality

Invisibility is achieved in this technique, by restricting modification to only the LSB. The embedding rate is 1 bit per pixel. The quality of the watermarked image is good with PSNR at 54 dB. Unlike the previous techniques the authentication and recovery bits are embedded in the ROI as well as RONI.

This scheme will be unacceptable in applications where there must be no modification to the image, and in such cases the watermarks could be embedded into a RONI if such a suitable region exists. It is clear that the image is modified, but the effect is minimal and such a change should be imperceptible to clinicians and would not affect diagnostic accuracy. There are currently no standards or guidelines for acceptable changes to watermarked images. Acceptable limits could be determined through clinical validation. This would require comparison of a sufficiently large number of images by separate clinicians to determine whether perceptible differences exist between images with and without watermarks and if such differences affect clinical decisions.

The design of such a study is described in Appendix A, but it was beyond the scope of this work to carry the study out.

- Security

The strength of this technique depends on the key and the use of k < Nb may not provide sufficient security. For an 800 x 600 image, there are approximately 1600 keys. This can easily be defeated with brute force attack. Using k > Nb will result in loss of key uniqueness, where more than one key can produce equivalent watermarks for the same image.

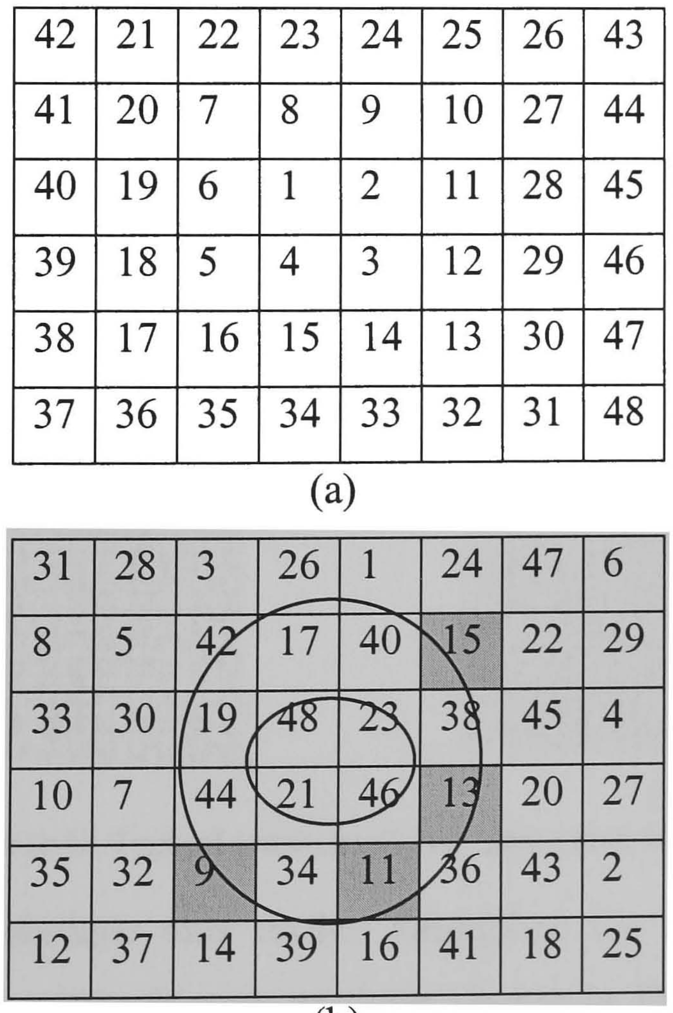
- Tamper detection and tamper localization

Tamper detection depends on the probability of getting the parity bit, *p* and average intensity, *v*. The probability of miss for level 1 detection is ½ x ½ = ¼ = 0.25. So the probability of missing detection for 6x6 block at level 2 detection would be $(\frac{1}{4})^4$ = 1/256 = 0.0039. For level-1 detection, if the type of error is parity error, then we are sure that the sub-block is indeed tampered. For level-2 detection, if the type of error is an intensity relationship error, we cannot be sure whether the sub-block under inspection is tampered with or other sub blocks within the same block are tampered. However, some pixels within the block must be in error. Thus, in case the tampered sub-block is not detected in level 1 inspection, the whole block will be marked tampered after level 2 inspections.

From the experimental results in Table 5.2 we find that the maximum missing rate after level-1 detection is 16% (probability of 0.16) and after level 2 detection is 0.1%. From the results, we can conclude that our method can detect tamper of size 3 x 3 pixels with a probability of 0.84 and tamper of size 6 x 6 pixels with a probability of 0.99. Using a mean intensity parity bit , it also ensures that we do not have a false alarm.

- Reconstruction

Reconstruction is achieved by embedding the recovery bits in a block some distance away from the original block as suggested by Fridrich and Goljan (1999). From the experimental results, it showed that the recovery bits were not embedded in blocks situated in the same column, but with some percentage in the same row. Those in the same row must have an odd distance from the original, because the way we spread the tamper was by using the same size, as the block use for embedding and the distance from each other were at least one block. If we change the tamper block size in the spread-tampered blocks, then we may have a different result.



42	21	22	23	24	25	26	43
41	20	7	8	9	10	27	44
40	19	6	1	2	11	28	45
39	18	5	4	3	12	29	46
38	17	16	15	14	13	30	47
37	36	35	34	33	32	31	48

(a)

31	28	3	26	1	24	47	6
8	5	42	17	40	15	22	29
33	30	19	48	23	38	45	4
10	7	44	21	46	13	20	27
35	32	9	34	11	36	43	2
12	37	14	39	16	41	18	25

(b)

Figure 6.3 (a) Spiral numbering of blocks (b) mapping with k=23, shaded blocks will not be recovered for 4x4 blocks tamper

We could also change the way we order the block number. Will it make a difference in the distribution of blocks? For example we could start the block at the centre and move in a spiral manner.

We anticipate the tamper is likely to be in the middle as the feature of ultrasound images has the region of interest in the middle. Our preliminary results show that the block spiralling and starting in the middle will have a greater chance of recovery compared to our proposed method. If we tamper with the 2x2 block in the middle, we will have two blocks that cannot be recovered, giving us 2/4 =50% recovery rate (refer to Figure 5.12(b)). With the spiral method we will have a 100% recovery for 2x2 block tamper in the middle of the image as in figure 6.3(b). If we have 4x4 blocks tampered, the proposed method will only have a 5/16 = 31% recovery rate, while the spiral method will give a higher recovery rate of 12/16 = 75%.

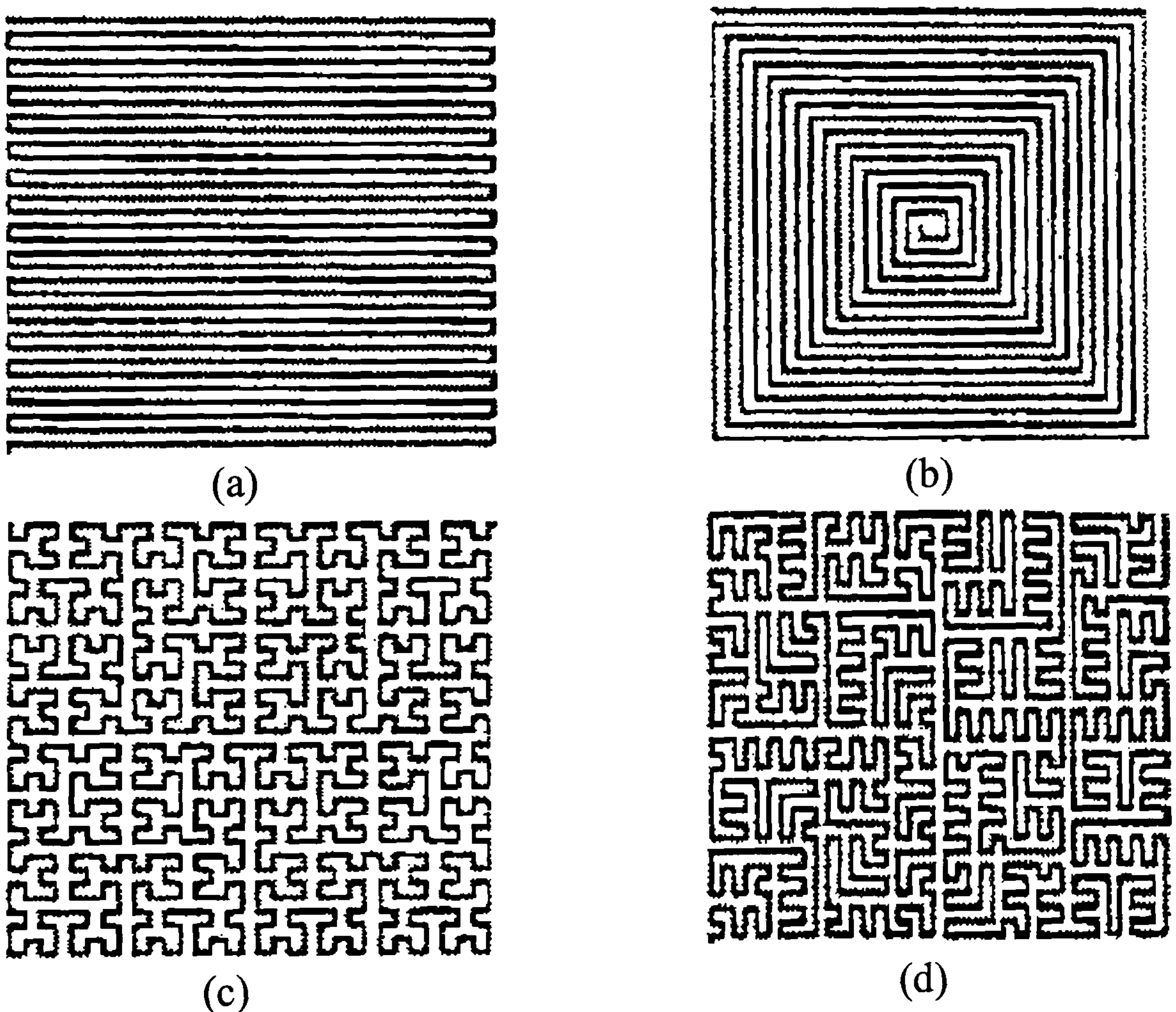


Figure 6.4 (a-b) Typical scans, (c-d) Key generated Peano scan

Considering the scan technique may further strengthen the method. In place of the simple raster scan, other methods such as those shown in Figure 6.4 could be used. Figure 6.4(a) is a reverse raster scan and appears to offer few advantages. Figure 6.4(b) is a spiral scan. Although advantageous for blocks in the middle, it retains the weaknesses of raster scan at the edges. The scan method of Figure 6.4(c) is the so-called Peano scan with the Peano-Hilbert variant shown in Figure 6.4(d). These are localised scan methods and could ensure blocks are relocated a minimum distance away. However, work on scanning has been conducted before and applied in other fields of research. The type of ordering or scanning called the Peano-Hilbert plane-filling curve as shown in figure 6.4(d) has been applied in a compression technique by Lempel and Ziv (1986). The possibilities of using the Peano-Hilbert scan for our watermarking technique can be explored further to find the optimal recovery point.

- VQ counterfeiting attack

The scheme is considered to be robust against a VQ counterfeiting attack by adding another level of authentication. Although the attack will successfully defeat level-1 and level-2 inspection, the attack will not survive level-3 detection (Section 5.5.3) as long as the key is kept secret.

6.6 Final proposal for AW-TDR

This section presents the final proposal for AW-TDR, describing the preparation of blocks, the embedding algorithm and the location plan for authentication bits and recovery bits.

Figure 6.5 shows the preparation of blocks B for embedding authentication bits and blocks C for embedding recovery bits. Blocks B will be mapped on to blocks C using an invertible function, as described in chapter 4 and chapter 5. Blocks B and C can be of different sizes.

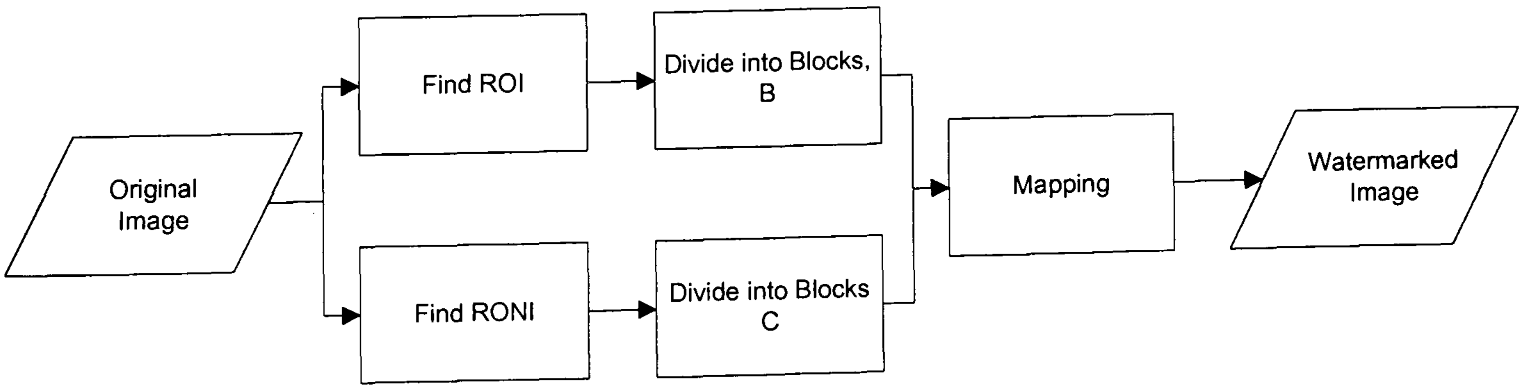


Figure 6.5 Mapping blocks in RONI for intensity embedding

Figure 6.6 shows the final proposal for the embedding algorithm for AW-TDR. The difference to the earlier version is that only the ROI is considered for the authentication process. The rest of the image will be used to embed the recovery bits.

Figure 6.7 shows the authentication bits, v and p will be embedded in the ROI and the recovery or reconstruction bits will be embedded in the RONI. We suggest the block size in ROI to be 4 x 4 pixels, with a sub-block of 2 x 2 pixels and the block size in RONI where the recovery bits to be embedded to be 2 x 1 pixels.

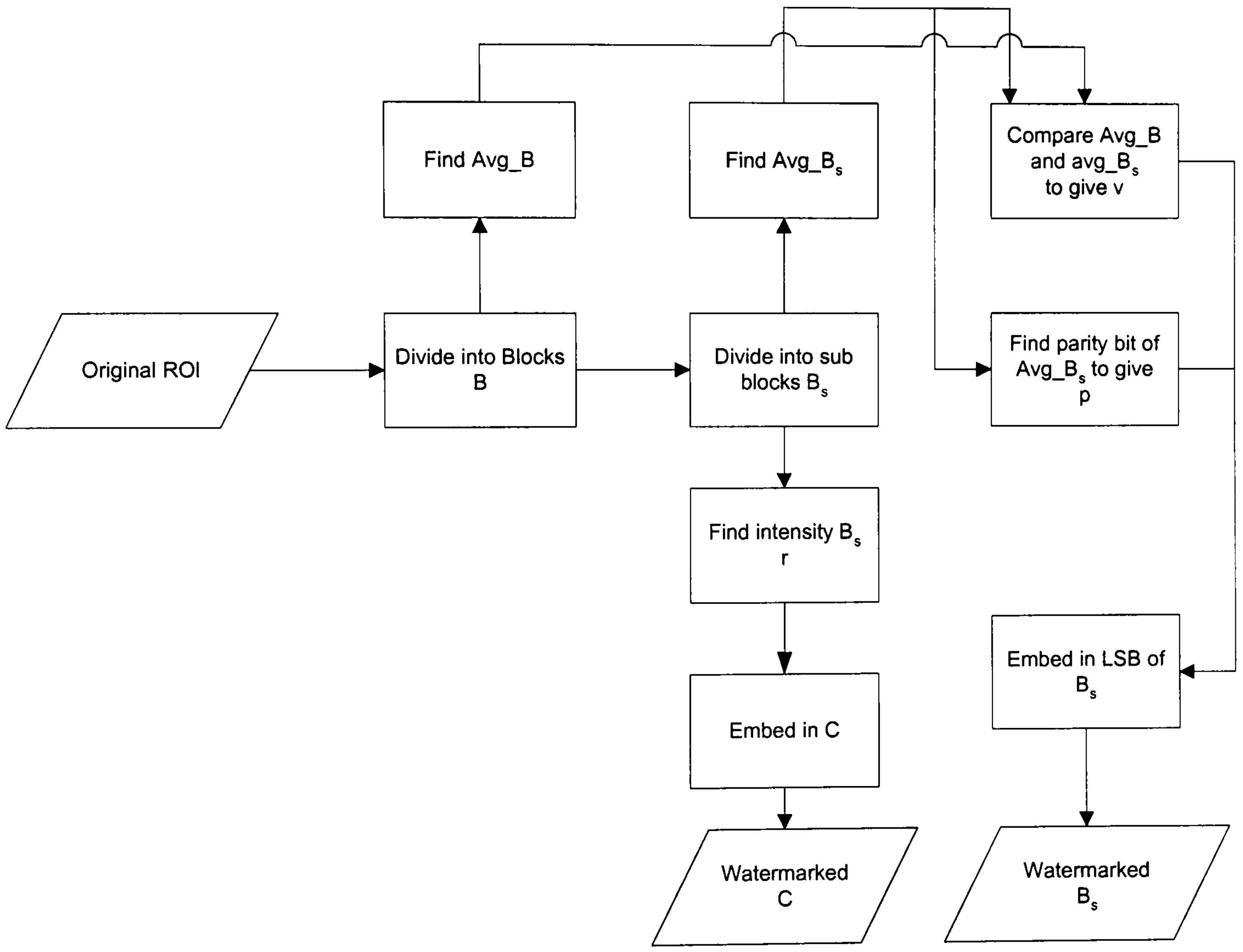


Figure 6.6 Final AW-TDR embedding

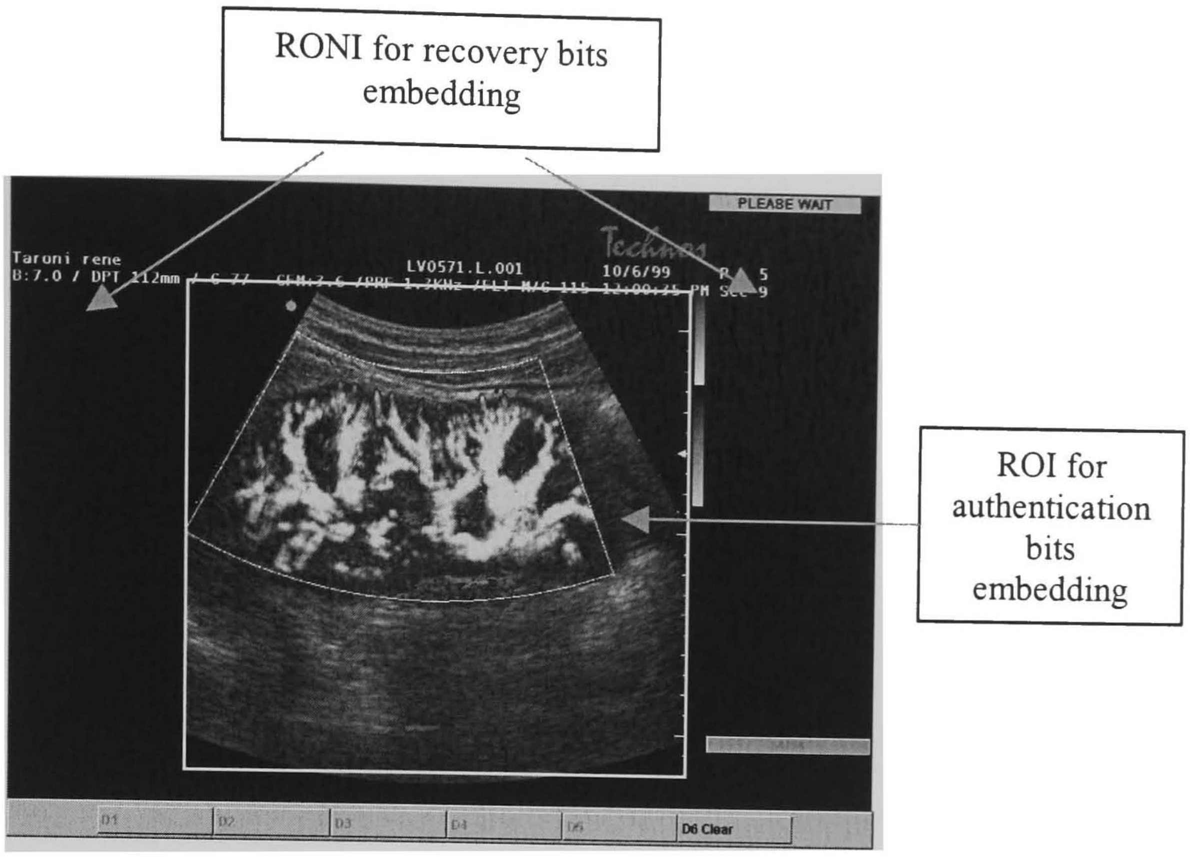


Figure 6.7 Location of bits for embedding

Figure 6.8 shows the location of the authentication bits, v and p in the LSB of pixels *p1* and *p2* respectively. The recovery bits, $r = r1r2r3r4r5r6r7$, form a seven-bit value that is the average of the sub-block, Bs. The seven bits *r1, r2, r3 and r4* are then embedded in the four LSBs of pixel *c1* and *r5, r6 and r7* are embedded in the four LSBs in pixel *c2*. For example if $p1 = 153$, $p2 = 155$, $p3 = 200$ and $p4 = 180$, $r = 172 = 10101100_2$. If *c1* and *c2* is 0 initially, *c1* will be 1010 and *c2* will be 1100 after embedding.

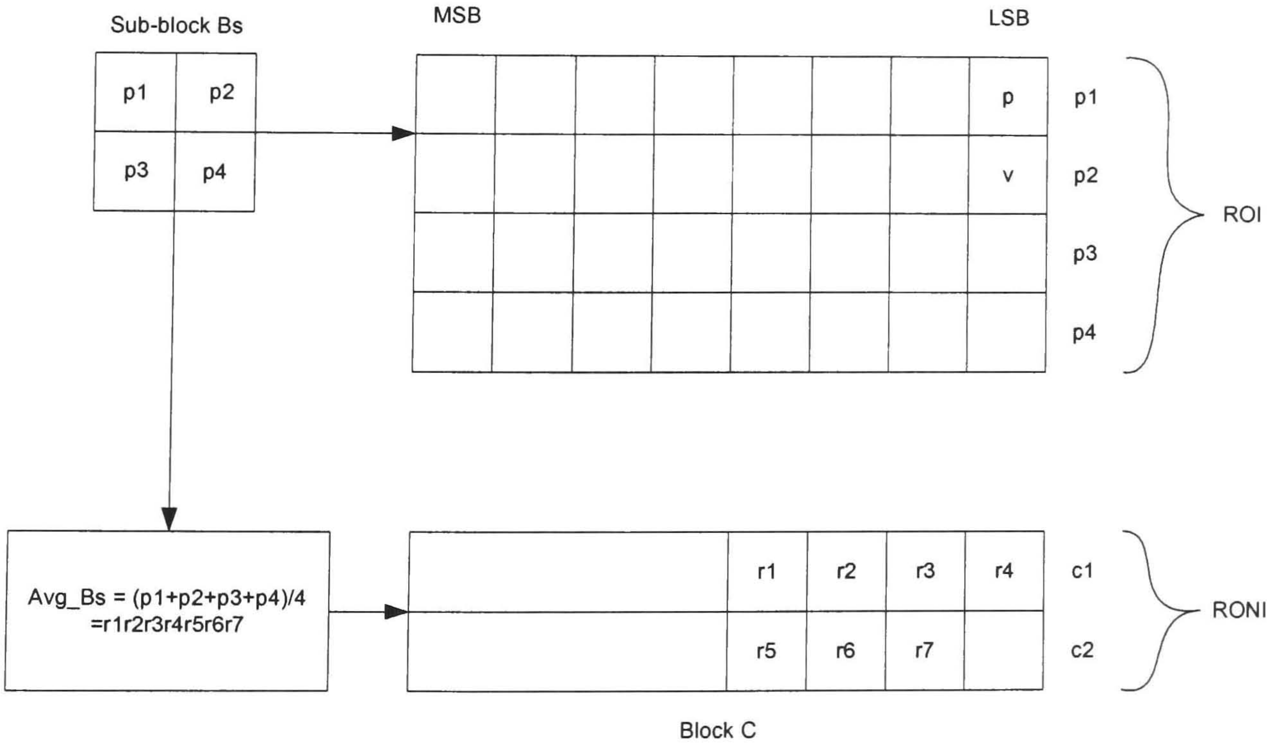


Figure 6.8 Location of bits in the corresponding pixels

The final proposal will enhance AW-TDR in three aspects:

1. Image quality in the ROI will be improved as the maximum change is only 2 bits in every 4 pixels, or embedding rate of 0.5 bits/pixel
2. Recovery rate will also be better since the recovery bits are located outside the region of interest. The disadvantage is that, only manipulation done in the ROI will be detected
3. The quality of the reconstructed image will be enhanced since the average of 2 x 2 pixels (please refer to figure 5.10) would be used to reconstruct the tampered image.

6.6 Summary

This chapter reviewed and evaluated the proposed schemes SAW, SAW-JPEG and AW-TDR.

SAW, a reversible watermarking scheme being capable of verifying authenticity and integrity of ultrasound images is proposed. It also allows recovery of the original image at the receiver. The SAW embedding scheme has a high capacity for embedding a watermark, in ultrasound images at around 1.06 bits/pixel. This makes the scheme superior to that of Guo and Zhuang (2003), which had an embedding rate of 0.0054 bits/pixel. Since the watermark is embedded in RONI, potentially an even higher embedding rate could be achieved.

SAW-JPEG is also a strict-authentication watermarking scheme and is robust to certain levels of JPEG compression. This work appears unique and there are no reports of embedding a watermark in the LSB to be robust against JPEG compression. This is because it is almost impossible for any image to survive their least significant bits after the quantization process. This technique is only unique to images with some areas of constant pixel values such as in ultrasound images. The method is based on exploiting the image feature that is able to survive compression and so may be modified to be robust over other compression schemes.

	Requirements	SAW	SAW-JPEG	AW-TDR
MANDATORY	Invisibility	Yes	Yes	Yes
	Detect tamper	Yes	Yes	Yes
	Security	Key	Key	Key
DESIRABLE	Reversibility	Yes	Yes	No
	Compression	No	Yes	No
	Localise tamper	No	No	Yes
	Reconstruction	No	No	Yes
OTHER	Distortion	2.6 x 10^6 dB	6.1 x 10^4 dB	54 dB

Table 6. 1. Summary of proposed watermarking

AW-TDR is a watermarking scheme that can detect and localise tamper and recover the image. The experimental results demonstrate that the precision of tamper detection and localisation is close to 100% after level-2 detection. The tamper recovery rate is better than 86% for a less than half tampered image.

The three schemes have been implemented on ultrasound images and the results have shown to be successful authentications of ultrasound images with the respective capabilities shown in Table 6.1. The mandatory requirements for watermarking identified in Table 2.2 were met and additional functionalities were developed.

From the evaluation and comparison of the three schemes proposed, this chapter determines current weaknesses and proposes modifications for enhanced versions. This includes modifying SAW-JPEG for blind authentication and a scheme for AW-TDR to have minimal embedding in the ROI.

Chapter 7

Conclusions and Reflections

7.1 Introduction

This chapter is structured as follows:

- Section 7.2 summarises the research
- Section 7.3 highlights the contributions and limitations of this thesis
- Section 7.4 gives suggestions for continuing the research in future work
- Section 7.5 summarises this chapter
- Section 7.6 reflects on the PhD process

7.2 Summary of Research

While the purpose of fragile watermarking and digital signature systems are similar, watermarking systems offer several advantages compared to signature systems (Memon et al. 1999) at the expense of requiring some modification (watermark insertion) of the image data. As a watermark is embedded directly into the image data, no additional information is necessary for authenticity verification. This is unlike digital signatures, since the signature itself must be bound to the transmitted data. The critical information needed in the authenticity testing process is discreetly hidden and more difficult to remove than a digital signature, or even if it is removed, it remains possible to detect that it has been tampered with. Also, digital signature systems view an image as an arbitrary bit stream and do not exploit its unique structure. Therefore a signature system may be able to detect that an image had been modified but cannot characterise the alterations. Many watermarking systems can determine which areas of a marked image have been altered and which areas have not, as well as estimate the nature of the alterations.

7.2.1 Summary

The advantages of watermarking compared to digital signature may be summarised as:

- No additional information/overhead needed
- Able to localise tamper or alterations
- Able to restore tampered images

The topic of watermarking in medical images has received relatively little research and analysis of the literature identifies that works remains to be undertaken on:

- Methods that can be used to solve the problem of watermarking medical images
- Methods that can be used to detect tampering
- Methods that can be used to recover tampered images

It is proposed that watermarking is reversible or conducted in the region of non-interest to make sure it will not change the diagnosis. This research is concerned with the issue of authenticating medical images. The issue of tamper detection and recovery are also of interest in this research.

7.2.2 Statement of the Problem

A major concern of the users of medical digital images is that it would be easy to modify the contents. Current cryptography methods can detect tampering by generating an authentication for the image, but at the expense of an overhead for its storage. It may also be separated from the image.

The aim of this research was to develop a method where the authentication may be embedded within the image itself - digital watermarking. The work considered watermarking methods that might be robust against the effect of applying lossy compression (e.g. JPEG) to such images. The methods were then enhanced to provide information on the location of the tampering and have an ability to return an approximate rendering of original image.

7.2.3 Purpose of the Study

The purpose of this study was to investigate and develop watermarking techniques suitable for medical imaging. This includes:

- The development of watermarking algorithms for:
    - Strict authentication
    - Strict authentication with JPEG compression
    - Tamper detection and recovery
- An implementation of the techniques on selected medical image modality.

7.3 Contributions and Limitations

The contributions of this thesis will be highlighted from each proposed scheme; Strict Authentication Watermarking (SAW), Strict Authentication Watermarking with JPEG Compression (SAW-JPEG) and Authentication Watermarking with Tamper Detection and Recovery (AW-TDR).

- Strict Authentication Watermarking (SAW)

The contributions of this scheme (SAW) cover three different elements of the research process: theory, practice and outcome. The integration of the digital signature as the watermark, the use of region of non-interest together with random mapping as the watermarking region is a novel approach in authentication watermarking. The scheme detects tamper by comparing the signature produced by hashing the region of interest. Any changes inside the area will have a significant change in the signature produced by the hash function. The system however will not detect changes made outside the region of interest. If this is of concern, then the system can be made to produce a signature of the whole image, which is embedded in the region of non-interest. At the receiver's side the watermark, which is the signature, is extracted and reverts the values to the original state. The signature is then calculated and compared to the received version.

Reversible watermarking for ultrasound images provides a lossless authentication watermark, which ensures the integrity of the image data without permanent loss of image fidelity. The reversibility is achieved by exploiting the characteristic of the ultrasound image. The abundance of redundant areas outside the region of interest with pixel values of zeros helps to achieve reversibility without having to employ a sophisticated technique and again is unique from studies reported in the literature

The SAW embedding scheme achieves a high capacity for watermarks to be embedded. Table 4.3 shows that 510,000 bits could be embedded in an 800x600x8 image with distortion less than 32 dB. This gives an embedding rate of 1.06 bits/pixel. This makes the scheme superior to that of Guo and Zhuang (2003) where their embedding rate is 0.0054 bits/pixel. In applications where the watermark is embedded in a RONI, potentially an even higher embedding rate could be achieved.

- Strict Authentication Watermarking with JPEG Compression.

The contribution that emerges from SAW-JPEG is an embedding technique in the LSB that can survive JPEG quantization process. The use of knowledge of the quantization algorithm to allow the DC coefficient to be unchanged through the compression/decompression process is used for the proposed watermarking scheme. There has been no attempt in studies from the literature to embed watermark in the LSB to be robust against JPEG compression before, as it is almost impossible for any image to survive their least significant bits after quantization process.

The SAW-JPEG technique uses informed authentication, that is it calculates the digital signature using information from the original image. In order to authenticate, the received digital signature should be compared against a new digital signature calculated from the original image. In telemedicine applications, the original image may not be available and so the digital signature must be found for the received image and compared to the received digital signature. The new scheme is shown in Figure 6.2.

- Authentication Watermarking with Tamper Detection and Recovery (AW-TDR)

AW-TDR is an efficient and effective digital watermarking method for image tamper detection and recovery. The contribution of this method is the integration of four concepts derived from the literature; 1) block-based (Fridrich and Goljan 1999); 2) separating authentication bits and recovery bits (Lin and Chang 2001); 3) hierarchical (Celik et al 2002); and 4) average intensity as image feature (Lou and Liu 2000). The method is efficient as it only uses simple operations, such as a parity check and comparison between average intensities. It is effective because the scheme inspects the image hierarchically with the inspection view increasing along with the hierarchy so that the accuracy of tamper localisation can be ensured. This scheme can perform both tamper detection and recovery for tampered images. Tamper detection is achieved through a block-based, inspection and recovery of a tampered block. It relies on its feature information hidden in another block that can be determined by a one-dimensional transformation.

The scheme is considered to be robust against a VQ counterfeiting attack by adding another level of authentication. Although the attack will successfully defeat level-1 and level-2 inspection, the attack will not survive level-3 detection (Section 5.5.3) as long as the key is kept secret.

A modification for AW-TDR to have minimal embedding in the ROI was proposed. The final proposal will enhance AW-TDR in three aspects:

1. Image quality in the ROI will be improved as the maximum change is only 2 bits in every 4 pixels, or embedding rate of 0.5 bits/pixel

2. Recovery rate will also be improved since the recovery bits are located outside the region of interest. The disadvantage is that only manipulation done in the ROI will be detected
3. The quality of the reconstructed image will be enhanced since the average of 2 x 2 pixels (please refer to figure 5.10) would be used to reconstruct the tampered image.

Limitations:

- SAW and SAW-JPEG are only applicable to images with RONI (e.g., ultrasound images).
- SAW and SAW-JPEG do not allow any bit change in the ROI. This implies that any legitimate image processing that changes the spatial value of the image will result in the image being considered as tampered.
- Security of AW-TDR depending on keys only. The use of k < Nb may not provide sufficient security. For an 800 x 600 image, there are approximately 1600 keys, which can easily be defeated with a severe attack.
- The three proposed schemes only consider LSB as the watermarking domain and so remain as fragile schemes
- AW-TDR is designed to detect local manipulations such as cut and paste, repainting and erasing. Global manipulations such as compression will result in the whole image is considered tampered.

Table 7.1 shows the summary of the contributions from the thesis.

Research Process	Contribution
Theory	1. The integration of a digital signature as a watermark and region of non-interest and random mapping as embedding area. 2. The use of an image feature for reversible watermarking. 3. The use of knowledge of the quantization algorithm to allow the DC coefficient to be unchanged through the compression/decompression process for watermarking. 4. The integration of four concepts introduced from the literature; block-based; separating authentication bits and recovery bits; hierarchical detection; and average intensity as image feature for detection and recovery.
Practice	1. Development of a scheme that is able to authenticate medical images with reversible capability. 2. Development of a scheme that is able to authenticate medical images and can survive a certain level of JPEG compression. 3. Development of a hierarchical scheme that is able to localise tamper with recovery capability.
Outcome	1. Strict Authentication Watermarking (SAW) 2. Strict Authentication Watermarking with JPEG Compression (SAW-JPEG) 3. Authentication Watermarking with Tamper Detection and Recovery (AW-TDR)

Table 7.1 Thesis Contributions

7.4 Further Research

The research has opened up a number of possibilities for future work. The suggested list is provided below:

- Improvement on security for AW-TDR. The use of k < Nb may not provide sufficient security. For an 800 x 600 image, there are approximately 1600 keys, which can easily be defeated with a severe attack.
- A variety of different error correction codes can be applied to improve on the quality of recovery bits (e.g., Hamming codes, turbo codes, and trellis codes). This metadata can be represented as a watermark. For example, a Reed Solomon ECC code can be used to generate parity bytes for each row and column of an image (Lee and Won 1999, Lee and Chen 2002). These parity bytes can be embedded as a watermark in the two significant bit planes of the image.
- To include reversible watermarking techniques, for example the one proposed by Goljan et al (2001) and at the same time maintain tamper detection and recovery for authentication bits embedded in the ROI.
- The possibilities of using the Peano-Hilbert scan for the AW-TDR watermarking technique can be explored further to find the optimal recovery point.
- As compression is acceptable in a medical standard such as DICOM, investigation on embedding in other domains such as DCT (used in JPEG) and wavelet (used in JPEG2000) should be considered to make sure the watermark is robust against those compression schemes.
- As in a radiology image lossy compression (Wong et al 1995), there exists no legal standards for regulating how much distortion induced by watermarking system can be accepted. To be acceptable, a watermarking system requires thorough clinical validation tests. Such tests must be carried out on a large number of images and should involve a number of clinicians to assure the diagnostic accuracy is not jeopardised by such distortion. We propose a study in Appendix A to find out whether or not our watermarking scheme interferes with clinical diagnosis.
- Application on other image modalities such as computed tomography (CT), magnetic resonance imaging (MRI), positron emission tomography (PET), single photon emission computerised tomography (SPECT), nuclear medicine (NM), digital subtraction angiography (DSA), and digitalflurography (DF).

- Issues in practical application in a real-world hospital environment need to be investigated before watermarking could possibly be used.

7.5 Summary

This research has demonstrated that watermarking can provide authentication for medical images. Three fragile watermarking schemes SAW, SAW-JPEG and AW-TDR have been investigated.

This research has extended current technology in fragile watermarking by providing a high capacity, reversible authentication service for medical images. SAW-JPEG demonstrates a technique to embed information in the LSB that can survive JPEG quantization process.

A hierarchical image authentication watermark (AW-TDR) is proposed that is able to validate the source of the image, verify its integrity, and when the integrity verification fails, determine the altered image regions. This approach overcomes the security problems associated with previous independent block-based authentication watermarks, while retaining their tamper localisation properties. The algorithm has been shown to provide security against vector-quantization (collage) counterfeiting attacks and accurate localisation of altered image regions.

Three schemes have been implemented on ultrasound images and the results have shown successful authentication of ultrasound images with the respective capabilities shown in table 6.1. The mandatory requirements for watermarking, identified in Table 2.2, were met with some additional functionality.

From the results and evaluation, it can be concluded that this research has met the objectives outlined in chapter 1.

7.5.1 Watermarking Future

Watermarking is still not a fully mature and understood technology, and many questions remain unanswered. However, the interest in watermarking is high, both from the academia and industry. The interest from academia is reflected in the number of publications on watermarking and in the number of conferences being held on watermarking and data hiding. The interest from industry is evident from the number of companies that have funded research in the field.

There exist enough applications where watermarking can provide working and successful solutions. Specifically for audio and video, it seems that watermarking technology will become widely deployed (MusicTrace 2005). The DVD industry standard, for example, will use watermarking for copy protection system (DRM Watch Staff 2004). Similarly, plans exist to use watermarking for copy protection for Internet audio distribution. Broadcast monitoring using watermarking is another application that will probably be widely deployed for both audio and video (Digimark 2001). Whether the development of watermarking technology will become a success story or not, remains to be seen, but it is a research area that is fast developing.

7.6 Personal Remarks

7.6.1 My PhD Journey

I am a lecturer at a university in Malaysia. I started my PhD when I was 35 years old, married with 5 children. It was not a straightforward decision to do a PhD. Although the university encourages people to do their PhD as early as possible in order to increase and enrich research activities in the country. A decision to leave your home for a period of over 3 years has to be based on a strategic plan as it will not only involve me, as the PhD candidate, but my family members too. So the initial plan was I would pursue my PhD, my husband will pursue his sub-specialty and three of the children would follow us.

I arrived in London in January, when the temperature was below 10 degree Celsius. It was soaring 33 degree at home! My first worry was the thought that I will not survive in this weather, not the PhD. We went through the immigration office who asked some absurd questions such as 'How much money do you have?' and 'Are you going back to your country after you have completed your studies?' The impression we got was that we are not welcome here. My first big hurdle was to find suitable accommodation for a family with three children. Many landlords turned us down because we have children. Once we lost our deposit money to an agent when the landlord did not allow us to move in at the last minute. We felt as if the system in this country was all against us. I felt like taking a drastic decision to quit the idea of doing a PhD. We eventually found accommodation after 3 tearful weeks with the help of a colleague from the department. We have to make do with a small space.

Being in a different country having a different culture is difficult, but it also enriches our learning process. Those experiences make us stronger as a person. I learnt that I had to take responsibility for my own learning. I was not used to deciding for myself. I felt lost, like being left in a forest and asked to find my own way. I would ask 'But where should I go?' and 'what path should I choose?' Nobody can answer those questions for me.

The process of completing the PhD took me through a series of emotions, not just the mental vigour to grasp what other people were doing in your field and to find out methodologies and approaches in trying to answer your questions. I will not forget incidences such as the Iraq war since March 2003, the Tsunami in December 2004 and recently the London bombings of 7th July 2005. I am writing them here because they have affected me in many ways and these events keep coming back to my mind when I sat writing this thesis.

So what will happen to me after the PhD? I will return to the university that sponsored me, Kolej Universiti Kejuruteraan Teknologi Malaysia (KUKTEM). Hopefully I will be able to pursue the research area of digital watermarking in medical images. I have already established contacts with radiologists from the Medical Faculty of the

International Islamic University Malaysia to become collaborators for the clinical evaluation of watermarked images. The hospital will be implementing teleradiology, so there will be medical images transferred across the network. The appropriate ethical approval will be sought from the university's ethic committee when I return to Malaysia.

7.6.2 My Conclusion on Security of Medical Images

A few people have asked me, "Why do you need to watermark medical images?" and a few others have asked me, "Who would want to forge medical images?". Here I will try to answer these two questions.

There is public concern regarding medical images being viewed and used by inappropriate parties, including relatives. This is of particular concern in telemedicine applications (Tachakra et al 1996) where images are shared outside a single organisation. Watermarking offers a method to embed patient details within an image, but in a way invisible to unauthorised persons. This may go some way to address these issues.

The approach taken in developing security techniques usually sees everybody as a potential criminal. This is really pathetic as the reasons behind it can be fictitious. This is to me like waiting in the battlefield waiting for an enemy that may never exist. To answer the second question, I could make a few fictitious criminals - the manipulation that can be achieved by adding or removing some parts of the image. The first person could be someone who wants to make false insurance claim by forging a medical image. The second person sells a forged medical image of a famous person to a tabloid newspaper. The third person is really vicious; he/she is trying to get away from his/her crime (homicide) by not just forging medical images, but the whole medical data to show that the death is through natural causes. But who gives them access to the data? An unauthorised person having access to the data, meaning that all security measures have failed. These include access to the building, to the room where the computer is located, the hospital network and the server where the data is stored. Planning to break all of these security measures require a lot of resources. Maybe it is cheaper and easier to bribe a person who has access to the file than to break the code. I shall leave this to the scriptwriter to keep the suspense.

A technology solution to provide privacy, confidentiality and security of medical data is important. However, technology can do very little to ensure that the person receiving information will handle it according to standards. That depends on ethics and an effective supervision and legal structure that provides sanctions against detected misuse. As the demand for sophisticated IT in healthcare grew over US$25 billion in 2000 (Anderson 2000), technology must also be made comprehensible to the clinicians and medical personnel; otherwise they will resist it.

Glossary

Active attack Any attempt to thwart the purpose of a watermarking system by modifying content. This includes unauthorised removal and unauthorized embedding.

Adversary Anyone who attempts to thwart the purpose of a watermarking system. Depending on the application, adversaries might attempt a variety of attacks, including unauthorised removal, unauthorised detection and unauthorised embedding. Other terms from the literature that have been used for an adversary include pirate, hacker, attacker and traitor.

Asymmetric key watermarking Any method of watermarking in which embedding and detection require the use of different watermarking keys.

Authentication The process of verifying the integrity of a watermark or the watermarked image.

Blind Authentication Authentication without any knowledge of the original, unwatermarked content.

Cryptography The study and practice of keeping message secure.

Digital signature The digital equivalent of a traditional signature. They are used to verify the identity of the sender. A digital signature can be constructed by encrypting a one-way hash of a message with the sender's private key.

Discrete Cosine Transform (DCT) A transform commonly used in image and video compression. The basic functions in this transform are real-valued cosine waves.

Error correction code (ECC) A mapping of messages into sequences of symbols such that not every possible sequence represents a message. In decoding such a code, sequences that do not correspond to messages are interpreted as corrupted code words. By defining the mapping between messages and code words in an appropriate way, it is possible to build decoders that can identify the code word closest to a given, corrupted sequence.

Exact authentication Verification that every bit of a given image has remained unchanged. This is in contrast to selective authentication.

False negative A type of error in which a detector fails to detect a watermark in a watermarked image.

False positive A type of error in which a detector incorrectly determines that a watermark is present in an image that was never watermarked.

Fragile watermark A watermark that becomes undetectable after even minor modifications of the image in which it is embedded. These are unsatisfactory for most applications, but can be useful for authentication.

Hash function A mapping of a variable length string into a fixed-length string called a hash. Typically, the hash of a string is shorter than the original.

Imperceptible Undetectable by a human perceptual system. This is often defined statistically.

Information hiding The art and science of hiding information. The fields of steganography and watermarking are examples of information hiding, but the term covers many other subjects, such as anonymous communications and preventing unauthorized database inference.

JPEG Joint Picture Experts Group- JPEG is a standard image compression technique based on block DCT quantization. JPEG2000 is a multi-scale wavelet-based image compression standard.

Key management Procedures for ensuring the integrity of keys used in cryptographic systems. This can include key generation, key distribution and key verification.

LSB watermarking The practice of embedding watermarks by placing information in the least significant bits of the image.

Message authentication Code (MAC) A one-way hash of a message that is then appended to the message. This is used to verify that the message is not altered between the time the hash is appended and the time it is tested.

One-way hash A hash function reasonably inexpensive to calculate, but prohibitively expensive to invert. That is, given an input string, it is easy to find the corresponding output. However, given a desired output, it is virtually impossible to find a corresponding input string.

Reversible watermark A watermark that can be exactly removed from the watermarked image, thereby obtaining a bit-for-bit copy of the original unwatermarked image. Such watermarks are more commonly referred to as invertible or erasable.

Robustness The ability of watermarks to survive signal processing operations.

Security In watermarking, the ability of a watermark to resist intentional tampering. More generally, the ability of an entire system (which may incorporate watermarking) to resist intentional tampering.

Semi-fragile watermark A watermark that is fragile against certain distortions but robust against others. This is useful for selective authentication.

Steganography The art of concealed communication by hiding messages in seemingly safe objects. The very existence of a steganographic message is secret. This term is derived from the Greek words *steganos*, which means covered, and *graphia*, which means writing.

Watermark A general term that can refer to an embedded message, a reference pattern, a message pattern or an added pattern.

Watermark key A secret key or key pair used for watermark embedding and detection. A watermark key can be used in conjunction with a cipher key.

Watermarking The practice of imperceptibly altering an image to embed a message about that image.

References

ACHARYA, R., ANAND, D., BHAT, S. and NIRANJAN, U.C., 2001. Compact storage of medical images with patient information, *IEEE Transactions Information Technology in Biomedicine*, **5**, pp. 320-323.

ANDERSON, J.G., 2000. Security of the distributed electronic patient record: a case-based approach to identifying policy issues, *International Journal of Medical Informatics*, **60**(2), pp. 111-118.

BARNI, M., BARTOLINI, F., CAPPELLINI, V., PIVA, A. and SALUCCO, F., 2001. Text-based geometric normalization for robust watermarking of digital maps, *IEEE International Conference on Image Processing (ICIP) 2001, Oct 7-10 2001 Thessaloniki,* IEEE Computer Society, pp.1082-1085.

BENEDENS, O. and BUSCH, C., 2000. Towards blind detection of robust watermarks in polygonal models. *Computer Graphics Forum,* **19**(3), pp. 199-208.

BHATTACHARJEE, S. and KUTTER, M., 1998. Compression tolerant image authentication, *IEEE International conference on image processing*, **1**, Chicago, IEEE, pp. 435-439.

BRASSIL, J.T., LOW, S. and MAXEMCHUK, N.F., 1999. Copyright protection for the electronic distribution of text documents. *Proceedings of the IEEE,* **87**(7), pp. 1181-1196.

CAO, F., HUANG, H.K. and ZHOU, X.Q., 2003. Medical image security in a HIPAA mandated PACS environment. *Computerized Medical Imaging and Graphics,* **27**(2-3), pp. 185-196.

CELIK, M.U., SHARMA, G., TEKALP, A.M., 2002. Hierarchical watermarking for secure image authentication with localization, *IEEE Transactions on Image Processing,* **11**(6), pp.585-594.

CHAO, H.M., HSU, C.M. and MIAOU, S.G., 2002. A data-hiding technique with authentication, integration, and confidentiality for electronic patients records, *IEEE Transactions Information Technology in Biomedicine*, **6**, pp. 46-53.

CHO, Y., AHN, B., KIM, J.S., KIM, I.Y. and KIM S.I., 2001. A study for watermark methods appropriate to medical images, *Journal of Digital Imaging*, **14**(2) supplement 1, pp.184-186.

CLUNIE, D.A., 2000. Lossless compression of grayscale medical images - effectiveness of traditional and state of the art approaches, *Medical Imaging 2000 - PACS Design and Evaluation: Engineering and Clinical Issues, Feb 15-Feb 17 2000 Bellingham, WA, USA,* Society of Photo-Optical Instrumentation Engineers pp.74-84.

COATRIEUX, G., MAITRE, H., SANKUR, B., ROLLAND, Y. and COLLOREC, R., 2000. Relevance of Watermarking in Medical Imaging, *2000 IEEE EMBS Conf. On Information Technology Applications in Biomedicine, November 2000 Arlington, USA*, IEEE, pp. 250-255.

COX, I.J., MILLER, M.L. and BLOOM, J.A., 2002. *Digital Watermarking.* San Francisco, CA: Morgan Kaufmann Publishers.

DIFFIE, W. and HELLMAN, M.E., 1976. New directions in cryptography. *IEEE Transactions on Information Theory,* **22**(6), pp. 644-654.

DIGIMARK, 2001. Press Releases: Philips Digital Networks Licenses Digimarc Digital Watermark Patents for Video Broadcast Monitoring [Homepage of Digimarc Corporation], [Online]. Available: http://www.digimarc.com/about/release.asp?newsID=59 [October 24, 2005].

DOBBERTIN, H., 1996. The Status of MD5 After a Recent Attack. *Crypto Bytes*, **2**(2), pp. 1 and 3, available : ftp://ftp.rsasecurity.com/pub/cryptobytes/crypto2n2.pdf [June 6, 2005].

DRM WATCH STAFF, 2004. Philips Releases Turnkey System for DVD Watermarking [Homepage of DRM], [Online]. Available: http://www.drmwatch.com/drmtech/article.php/3427971 [October 24, 2005].

EGGERS, J.J., IHLENFELDT, W. and GIROD, B., 2001. Digital watermarking of chemical structure sets, *Proceedings of the 4th Information Hiding Workshop '01, 25-27 April 2001 Pittsburgh, PA, USA.*

FEDERATION BUREAU OF INVESTIGATION (FBI), October 2000, 2000-last update, forensic audio, video & image analysis unit [Homepage of FBI], [Online]. Available: http://www.fbi.gov/hq/lab/org/faviau.htm [May 6, 2005].

FRIDRICH, J., GOLJAN, M. and BALDOZA, A.C., 2000. New fragile authentication watermark for images, *International Conference on Image Processing (ICIP 2000), Sep 10-13 2000 Vancouver, BC,* IEEE Computer Society pp. 446-449.

FRIDRICH, J., 1998. Image watermarking for tamper detection, *Proceedings of the 1998 International Conference on Image Processing, ICIP. Part 2 (of 3), Oct 4-7 1998 Los Alamitos, CA, USA,* IEEE Comp Society, pp. 404-408.

FRIDRICH, J. and GOLJAN, M., 1999. Images with self-correcting capabilities. *IEEE International Conference on Image Processing,* **3**, pp. 792-796.

FRIEDMAN, G.L., 1993. The Trustworthy Digital Camera: Restoring Credibility to the Photographic image. *IEEE Transactions on Consumer Electronics,* **39**(4), pp. 905-910.

GARFINKEL, S. and SPAFFORD, G., 1996. *Practical Unix and Internet Security.* Devon, UK: O'Reilly & Associates.

GIAKOUMAKI, A., PAVLOPOULOS, S. and KOUTSOURIS, D., 2003. A medical image watermarking scheme based on wavelet transform, *Engineering in Medicine and*

Biology Society. Proceedings of the 25th Annual International Conference of the IEEE, Sep 17-21 2003 Cancun, Mexico, IEEE, **1**, pp. 856-859.

GIROD, B., 1993. What's Wrong with Mean-squared Error? In: Watson, A. B., ed. *Digital Images and Human Vision*, Cambridge, MA:MIT Press, pp. 207-220.

GOLJAN, M., FRIDRICH, J. and DU, R., 2001. Distortion-free data embedding for images, *Proceedings of 4th International Workshop on Information Hiding, Lecture Notes in Computer Science*, **2137**, pp. 27-41.

GREEN, D. M. and SWETS, J.A. 1974. *Signal Detection Theory and Psychophysics*, Huntington, New York: Robert E. Krieger Publishing Co.

GUO, X. and ZHUANG, T., 2003. A lossless watermarking scheme for enhancing security of medical data in PACS, *Medical Imaging 2003: PACS and Integrated Medical Information Systems: Design and Evaluation, Feb 18-20 2003 San Diego, CA, USA,* The International Society for Optical Engineering, pp.350-359.

HAWKES, P., PADDON, M. and ROSE, G.G., 2005, Musings on the Wang et al. MD5 collision [Homepage of International Association of Cryptologic Research (IACR)], [Online]. Available: http://eprint.iacr.org/2004/264.pdf [May 10, 2005].

HERNANDEZ, J.R., AMADO, M. and PEREZ-GONZALEZ, F., 2000. DCT-domain watermarking techniques for still images: detector performance analysis and a new structure. *IEEE Transactions on Image Processing,* **9**(1), pp. 55-68.

HOLLIMAN, M. and MEMON, N., 2000. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes. *IEEE Transactions on Image Processing,* **9**(3), pp. 432-41.

HONSINGER, C.W., JONES, P.W., RABBANI, M. and STOFFEL, J.C., 2001. Lossless recovery of an original image containing embedded data. Patent No. US06278791, United States.

HORII, S.C., 1997-last update, A nontechnical introduction to DICOM [Homepage of Radiological Society of North America], [Online]. Available: http://www.rsna.org/REG/practiceres/dicom/nontechintro.html [07/08, 2003].

HUANG, H.K., 2003. Enterprise PACS and image distribution. *Computerized Medical Imaging and Graphics,* **27**(2-3), pp. 241-53.

ITU, 2000. *Methodology for the Subjective Assessment of the Quality of Television Pictures: Recommendation ITU-R BT.500-10,* Radiocommunication Assembly.

JOHNSON, N.F. and KATZENBEISSER, S.C., 2000. A Survey of Steganographic Techniques, In: S. KATZENBEISSER and PETITCOLAS, FABIEN A. P., eds, *Information Hiding Techniques for Steganography and Digital Watermarking.* Norwood, MA: Artech House, pp. 43-75.

KUNDUR, D. and HATZINAKOS, D., 1998. Towards a telltale watermarking technique for tamper-proofing, *Proceedings of IPCIP'98 International Conference on Image Processing, 4-7 Oct. 1998 Chicago, IL, USA,* IEEE Computer Society, pp. 409-13.

KUNDUR, D. and HATZINAKOS, D., 1996. Blind image deconvolution. *IEEE Signal Processing Magazine,* **13**(3), pp. 43-64.

KUTTER, M. and HARTUNG, F., 2000. Introduction to watermarking techniques, In: S. KATZENBEISSER and PETITCOLAS, FABIEN A. P., eds., *Information Hiding Techniques for Steganography and Digital Watermarking.* Norwood, MA: Artech House, pp. 97-120.

KWON, K., KWON, S., LEE, S., KIM, T. and LEE, K., 2003. Watermarking for 3D polygonal meshes using normal vector distributions of each patch, *Proceedings: International Conference on Image Processing, ICIP-2003, Sep 14-17 2003 Barcelona, Spain,* IEEE Computer Society, pp. 499-502.

LANGELAAR, G.C., SETYAWAN, I. and LAGENDIJK, R.L., 2000. Watermarking digital image and video data. *IEEE Signal Processing Magazine,* **17**(5), pp. 20-46.

LEE, J. and CHEE SUN WON, 2000. Image integrity and correction using parities of error control coding, *IEEE International Conference on Multimedia and Expo (ICME 2000), Jul 30-Aug 2 2000 New York, NY, USA,* IEEE, pp. 1297-1300.

LEE, J. and WON, C.S., 1999. Authentication and correction of digital watermarking images. *Electronics Letters,* **35**(11), pp. 886-887.

LEE, W. and CHEN, T., 2002. A public verifiable copy protection technique for still images. *Journal of Systems and Software,* **62**(3), pp. 195-204.

LEMPEL, A., ZIV, J., 1986, Compression of two-dimensional data, *IEEE Transactions on Information Theory*, **32**(1), pp. 2-8.

LI, C., LOU, D. and LIU, J., 2003. Image integrity and authenticity verification via content-based watermarks and a public key cryptosystem. *Journal of the Chinese Institute of Electrical Engineering, Transactions of the Chinese Institute of Engineers, Series E/Chung KuoTien Chi Kung Chieng Hsueh K'an,* **10**(1), pp. 99-106.

LI, W. and XUE, X., 2003. An audio watermarking technique that is robust against random cropping. *Computer Music Journal,* **27**(4), pp. 58-68.

LIN, C.-. and CHANG, S.-., 2001. A robust image authentication method distinguishing JPEG compression from malicious manipulation. *IEEE Transactions on Circuits and Systems for Video Technology,* **11**(2), pp. 153-168.

LIN, C. and CHANG, S., 2000. Semi-fragile watermarking for authenticating JPEG visual content, *Security and Watermarking of Multimedia Contents II, Jan 24-Jan 26 2000 Bellingham, WA, USA,* Society of Photo-Optical Instrumentation Engineers, pp. 140-151.

LOU, D. C. and LIU, J. L., 2000. Fault resilient and compression tolerant digital signature for image authentication. *IEEE Transactions on Consumer Electronics*, **46**(1), pp. 31-39.

MACQ, B. and DEWEY, F., 1999. Trusted Headers for Medical Images, *DFG VIIII-DII Watermarking Workshop,* Erlangen, Germany.

MEMON, N., SHENDE, S. and WONG, P., 1999. On the security of the Yueng-Mintzer Authentication Watermark, *Final Program and Proceedings of the IS&T PICS 99, April 1999 Savannah, GA, USA*, The Society for Imaging Science and Technology, pp. 301-306.

MENEZES, A., OORCHOT P. VAN and VANSTONE, S., 1997. *Handbook of Applied Cryptography.* Boca Raton, FL:CRC.

MINTZER, F., BRAUDAWAY, G.W. and BELL, A.E., 1998. Opportunities for Watermarking Standards. *Communications of the ACM,* **41**(7), pp. 55-64.

MINTZER, F., BRAUDAWAY, G.W. and YEUNG, M.M., 1997. Effective and ineffective digital watermarks, *Proceedings of the 1997 International Conference on Image Processing. Part 3 (of 3), Oct 26-29 1997 Los Alamitos, CA, USA,* IEEE Comp Soc, pp. 9-12.

MONDEN, A., IIDA, H., MATSUMOTO, K., INOUE, K. and TORII, K., 2000. Practical method for watermarking Java programs, *2000 IEEE 24th Annual International Computer Software and Applications Conference (COMPSAC 2000), Oct 25-Oct 27 2000 Los Alamitos, CA, USA,* IEEE Computer Society, pp.191-197.

MURRAY, T.D., 1996-last update, the wizard of watermarks [Homepage of Virginia Tech.], [Online]. Available: http://ebbs.english.vt.edu/gravell/wizard/wizard.html [June 30, 2004].

MUSICTRACE, 2005. Watermark embedding for audio signals [Homepage of MusicTrace], [online]. Available: http://www.musictrace.de/products/contentmark.en.htm [October 24, 2005].

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION, 2003. *Digital Imaging and Communications in Medicine (DICOM).* PS 3.1-2003, available:

http://www.amicas.com/pacsed/DICOM%20Strategy_2002-03-28.doc [6 July 2004, 2004].

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 1995. *Secure Hash Standard (SHA-1).* Federal Information Processing Standards Publication #180-1, available: http://www.itl.nist.gov/fipspubs/fip180-1.htm [June 30, 2004].

OKADA, H., SHIITEV, A., SONG, H., FUJITA, G., ONOYE, T. and SHIRAKAWA, I., 2002. Error detection by digital watermaking for MPEG-4 video coding. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,* **E85-A**(6), pp. 1281-1288.

O'RUANAIDH, J.J.K. and PUN, T., 1997. Rotation, scale and translation invariant digital image watermarking, *Proceedings of IEEE International Conference on Image Processing, October 1997 Santa Barbara, CA, USA*, IEEE, (**1**), pp. 536-539.

PAQUET, A.H., WARD, R.K. and PITAS, I., 2003. Wavelet packets-based digital watermarking for image verification and authentication. *Signal Processing,* **83**(10), pp. 2117-2132.

PETITCOLAS, FABIEN A. P., 2000. Introduction to Information Hiding. In: S. KATZENBEISSER and PETITCOLAS, FABIEN A. P., eds., *Information Hiding Techniques for Steganography and Digital Watermarking.* Norwood, MA: Artech House, pp. 1-11.

RIVEST, R.L., April 1992. *The MD5 Message Digest Algorithm.* Internet Request For Comments: MIT Laboratory for Computer Science and RSA Data Security, Inc.

RIVEST, R.L., SHAMIR, A. and ADLEMAN, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM,* **21**(2), pp. 120-126.

SAID, A. and PEARLMAN, W.A., 1996. A new, fast, and efficient image codec based on set partitioning in hierarchical trees. *IEEE Transactions on Circuits and Systems for Video Technology,* **6**(3), pp. 243-50.

SCHNEIDER, M. and CHANG, S.F., 1996. Robust content based digital signature for image authentication, *Proceedings of IEEE International Conference on Image Processing, September 16-19 1996 Lausanne, Switzerland,* IEEE, **3**, pp. 227-230.

SHANNON, C.E., 1948. A Mathematical Theory of Communication, *Bell System Technical Journal,* **27**(4), 373-423, 623-656.

STALLINGS, W., 2003. *Network Security Essentials Applications and Standards.* Second ed. Upper Saddle River, New Jersey: Prentice Hall.

STINSON, D.R., 1995. *Cryptography: Theory and Practice.* Boca Raton, FL: CRC Press.

SU, J.K., HARTUNG, F. and GIROD, B., 1998. Digital watermarking of text, image, and video documents. *Computers & Graphics,* **22**(6), pp. 687-695.

SUN, S. and CHANG, P., 2003. Video watermarking synchronization based on profile statistics, *Proceedings: 37th Annual 2003 International Carnahan Conference on Security Technology, Oct 14-16 2003 Taipei, Taiwan,* IEEE, pp. 410-413.

TACHAKRA, S., MULLETT S.T.H., FREIJ, R. and SIVAKUMAR, A., 1996. Confidentiality and ethics in telemedicine, *Journal of Telemedicine and Telecare,* **2**(1), pp. 68-71.

TONG, LIU and ZHENG-DING, QIU, 2002. The survey of digital watermarking-based image authentication techniques, *Proceedings of International Conference on Signal Processing (ICSP), 26-30 Aug. 2002 Beijing, China,* IEEE, pp. 1556-1559.

TRICHILI, H., BOUHLEL, M., DERBEL, N. and KAMOUN, L., 2002. A new medical image watermarking scheme for a better telediagnosis, *Proceedings of IEEE International Conference on Systems, Man and Cybernetics, Oct 6-9 2002 Yasmine Hammamet, Tunisia,* IEEE, pp. 557-560.

TSAI, P., HU, Y. and CHANG, C., 2004. A color image watermarking scheme based on color quantization. *Signal Processing,* **84**(1), pp. 95-106.

UTKU CELIK, M., SHARMA, G., SABER, E. and MURAT TEKALP, A., 2002. Hierarchical watermarking for secure image authentication with localization. *IEEE Transactions on Image Processing,* **11**(6), pp. 585-95.

VAN SCHYNDEL, R.G., TIRKEL, A.Z. and OSBORNE, C.F., 1994. A digital watermark, *Proceedings of 1st International Conference on Image Processing, 13-16 Nov 1994 Austin, TX, USA,* IEEE Computer Society Press, pp. 86-90.

VOYATZIS, G. and PITAS, I., 1996a. Applications of toral automorphisms in image watermaking, *Proceedings of the 1996 IEEE International Conference on Image Processing, ICIP'96. Part 2 (of 3), Sep 16-19 1996 Los Alamitos, CA, USA,* IEEE, pp. 237-240.

VOYATZIS, G. and PITAS, I., 1996b. Chaotic mixing of digital images and applications to watermarking, *Proceedings of European Conference on Multimedia Applications, Services and Techniques, 28-30 May 1996 Louvain la Neuve, Belgium,* Univ. Catholique Louvain, pp. 687-94.

WAKATANI, A., 2002. Digital Watermarking for ROI Medical Images by Using Compressed Signature Image, *35th Annual Hawaii International Conference on System Sciences (HICSS-35'02), 7-10 Jan 2002 Big Island, Hawaii,* IEEE, pp. 2043-2048.

WALLACE, G.K., 1991. The JPEG Still Picture Compression Standard. *Communications of the ACM,* **34**(4), pp. 30-44.

WALTON, S., 1995. Information authentication for a slippery new age. *Dr. Dobbs Journal,* **20**(4), pp. 18-26.

WANG, X., FENG, D., LAI, X. and YU, H., August 2004, 2004-last update, collisions for hash functions MD4, MD5, HAVAL-128, and RIPEMD. Available: http://eprint.iacr.org/2004/199 [May 10, 2005].

WOLFGANG, R.B. and DELP, E.J., 1996. A watermark for digital images, *Proceedings of International Conference on Image Processing, ICIP'96, Sep 16-19 1996 Los Alamitos, CA, USA, IEEE,* **3**, pp. 219-222.

WOLFGANG, R.B., PODILCHUK, C.I. and DELP, E.J., 1999. Perceptual watermarks for digital images and video. *Proceedings of the SPIE - The International Society for Optical Engineering, Security and Watermarking of Multimedia Contents, 25-27 Jan. 1999 San Jose, CA, USA*, Society of Photo-Optical Instrumentation Engineers, **3657**, pp. 40-51.

WOLFGANG, R.B. and DELP, E.J., 1999. Fragile watermarking using the VW2D watermark. *Proceedings of SPIE - The International Society for Optical Engineering, Security and Watermarking of Multimedia Contents, 25-27 Jan. 1999 San Jose, CA, USA*, Society of Photo-Optical Instrumentation Engineers, **3657**, pp. 204-213.

WONG, P., 1999. A watermark for image integrity and ownership verification, *Final Program and Proceedings of the IS&T PICS 99, April 1999 Savannah, GA, USA*, The Society for Imaging Science and Technology, pp.374-379.

WONG, P.W., 1998. Public key watermark for image verification and authentication, *Proceedings of the 1998 International Conference on Image Processing, ICIP. Part 1 (of 3), Oct 4-7 1998 Los Alamitos, CA, USA,* IEEE Computer Society, pp. 455-459.

WONG, P.W. and MEMON, N., 2000. Secret and public key authentication watermarking schemes that resist vector quantization attack, *Security and Watermarking of Multimedia Contents II, Jan 24-Jan 26 2000 Bellingham, WA, USA,* Society of Photo-Optical Instrumentation Engineers, pp.417-427.

WONG, S., ZAREMBA, D., GOODEN, D. and HUANG, H.K., 1995. Radiologic image compression-a review, *Proceedings of IEEE*, **83(2)**, pp. 194-219.

WU, M. and LIU, B., 1998. Watermarking for image authentication, *Proceedings of the 1998 International Conference on Image Processing, ICIP. Part 2 (of 3), Oct 4-7 1998 Los Alamitos, CA, USA*, IEEE Computer Society, pp. 437-441.

XIE, L. and ARCE, G.R., 1998. Joint wavelet compression and authentication watermarking, *Proceedings of the 1998 International Conference on Image Processing, ICIP. Part 2 (of 3), Oct 4-7 1998 Los Alamitos, CA, USA,* IEEE Computer Society, pp. 427-431.

YAN, F., JI, B., ZHANG, D. and FANG, H., 2004. Robust quadri-phase audio watermarking. *Acoustical Science and Technology,* **25**(1), pp. 106-108.

YANG, Y. and BAO, F., 2003. An invertible watermarking scheme for authentication of electronic clinical brain atlas, *IEEE International Conference on Accoustics, Speech, and Signal Processing, Apr 6-10 2003 Hong Kong,* IEEE, pp.533-536.

YEUNG, M.M. and MINTZER, F., 1997. An invisible watermarking technique for image verification, *Proceedings of International Conference on Image Processing, Oct 1997 Santa Barbara, CA, USA*, IEEE, **2**, pp. 680-683.

YEUNG, M.M. and MINTZER, F.C., 1998. Invisible watermarking for image verification. *Journal of Electronic Imaging,* **7**(3), pp. 578-591.

ZHANG, X., FENG, J. and LO, K., 2003. Image watermarking using tree-based spatial-frequency feature of wavelet transform. *Journal of Visual Communication and Image Representation,* **14**(4), pp. 474-491.

ZHOU, X.Q., HUANG, H.K. and LOU, S.L., 2001. Authenticity and integrity of digital mammography images. *IEEE Transactions on Medical Imaging,* **20**(8), pp. 784-791.

ZHU, B., SWANSON, M.D. and TEWFIK, A.H., 1996. Transparent robust authentication and distortion measurement technique for images, *7th IEEE Digital Signal Processing Workshop Proceedings, Sep 1-4 1996 Loen, Norway*, IEEE, pp.45-48.