A novel CRT-based watermarking technique for authentication of multimedia contents

Karthik, A.; Patra, Jagdish Chandra; Bornand, Cedric

2009

Patra, J. C., Karthik, A., & Bornand, C. (2009). A novel CRT-based watermarking technique for authentication of multimedia contents. *Digital Signal Processing*, 20(2), 442-453.

<https://hdl.handle.net/10356/94341>

<https://doi.org/10.1016/j.dsp.2009.07.004>

© 2009 Elsevier. This is the author created version of a work that has been peer reviewed and accepted for publication by *Digital Signal Processing*, Elsevier. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [DOI: <http://dx.doi.org/10.1016/j.dsp.2009.07.004>].

Downloaded on 26 Apr 2023 21:43:26 SGT

A novel CRT-based watermarking technique for authentication of multimedia contents

Jagdish C. Patra^{a,*}, A. Karthik^a, Cedric Bornand^b

^a School of Computer Engineering, Nanyang Technological University, Nanyang Avenue, Singapore

^b HEIG-VD, University of Applied Sciences, Yverdon-les-Bains, Switzerland

A B S T R A C T

Digital watermarking techniques have been proposed as a solution to the problem of copyright protection of multimedia data. In this paper, we propose a novel Chinese remainder theorem (CRT)-based technique for digital watermarking. The use of CRT for this purpose provides additional security along with resistance to some familiar attacks. We have shown that this technique is quite resilient to addition of the noise. We have compared performance of the proposed technique with recently reported two singular value decomposition (SVD)-based watermarking techniques and shown its superior performance in terms of tampering assessment function (TAF), computational efficiency and peak signal to noise ratio (PSNR). For example, the embedding time of the proposed CRT-based scheme is 6 and 3 times faster than the SVD-based Schemes 1 and 2, respectively. This technique can also be applied to document, audio and video contents.

1. Introduction

Today's information driven economy is dominated by the tremendous growth of the Internet and explosion of day-to-day data processing with huge amount of multimedia data. Easy availability of content-editing software, mobile and compact digital devices and the Internet, make the digital lifestyle of common man quite different from that of few years ago. Digital multimedia contents, e.g., text, image, video and audio, can be easily altered, stored or transmitted to any point of the globe instantly. However, multimedia digital content owners are skeptical of putting their content on the Internet due to lack of intellectual property protection available to them. In order to address this situation, digital watermarking is indeed one of the solutions to protect the ownership of these contents. In digital watermarking techniques, some digital signature that is unique to the owner or copyright information is embedded into the host multimedia content. The signature embedded remains invisible and imperceptible and cannot be removed easily even under certain manipulations, e.g., addition of noise, compression, tampering and scaling operations. Only the authorized recipient of the digital content can extract the watermark from the watermarked content with the knowledge of some key information. In this way security, content integrity and intellectual protection can be provided to the owner. In this direction, starting from mid-1990, several researchers have reported many watermarking techniques in spatial and transform domains [1–3].

Some important properties of an effective watermarking scheme are [1–3]: (i) imperceptibility: there should not be any noticeable difference between a watermarked content and the original, (ii) robustness: the embedded watermark should be able to withstand to some extent of content manipulation. Any attempt to destroy a watermark should also void the watermarked content and (iii) trustworthiness: no other watermark other than the embedded watermark should be extracted

* Corresponding author.

E-mail addresses: aspatra@ntu.edu.sg (J.C. Patra), AL0001IK@ntu.edu.sg (A. Karthik), cedric.bornand@heig-vd.ch (C. Bornand).

from the watermarked content. This is to reduce ambiguity on the ownership of the content. Unfortunately, it is impracticable to design a technique, which features all the above mentioned qualities simultaneously. Therefore, it would be necessary to make tradeoffs on some of these qualities.

Based on the application and methods used, different types of watermarking techniques were exist.

- *Fragile/Robust watermark.* A fragile watermark authenticates images and documents. Such a scheme identifies and locates changes in the watermarked content. The robust watermark is different because it is integrated into the content and is supposed to be resistant to attacks.
- *Blind, Semi-blind, Non-blind scheme.* A blind scheme requires only a key for extraction of the watermark, where as in a semi-blind scheme, more information is required such as the watermark. Lastly, for the non-blind scheme, the host image is also needed for the extraction of the watermark.

The research in watermarking techniques covers a very wide area [1–3]. Many different techniques have been devised using cryptography and quantization-based embedding to improve security [4,5], discrete cosine transformation [6,7] to make use of properties in the frequency domain, and error control codes [8] to increase robustness. An independent component analysis-based blind watermarking technique with interesting results has been proposed in [9]. Many published schemes rely on similar principles or approaches, but they differ in their implementation methodology. Recently few singular value decomposition (SVD)-based elegant watermarking techniques have been proposed in [10–15].

In this paper, we propose a novel watermarking technique based on Chinese remainder theorem (CRT). The CRT has been used in several engineering problems, such as hierarchical access control by assigning cryptographic keys [16], secret sharing of stego-images [17], construction of quasi-cyclic codes [18], residue number systems [19] and oblivious data transfer mechanism [20]. A CRT-based watermarking scheme with preliminary results has been reported in [21]. However, there are not many applications of CRT for watermarking. The main purpose of using CRT in watermarking is its added security. For example, by selecting a set of relatively prime numbers $\mu = \{M_1, M_2, \dots, M_r\}$ and using CRT, a large integer Z can be represented by a set of smaller integers $\{R_1, R_2, \dots, R_i\}$. It is extremely difficult to get back the original integer Z without knowing μ . This fact provides additional security in this scheme. Since CRT is based on simultaneous congruences and modular arithmetic, it is computationally efficient. In addition, at the time of extraction of watermark, only a few information are needed. We have shown that the proposed technique introduces minimal distortion to the original host image, during embedding process and it can withstand the noise attack quite well. We have compared performance of the proposed scheme with the two recently reported SVD-based schemes, and shown its superior performance by conducting different attacks to the watermarked image. In this paper, we have also proposed a method to increase the watermarking capacity.

The rest of the paper is as follows. We briefly introduce the two existing SVD-based schemes in Section 2. The mathematics of CRT is introduced in Section 3. Next, the CRT-based watermarking scheme is explained in Section 4. The experimental results and performance comparison with SVD-based techniques have been included in Section 5. Finally, conclusions and discussions on this study have been made in Section 6.

2. Existing SVD-based watermarking schemes

In this section, we briefly discuss the two recently reported SVD-based watermarking schemes and their weaknesses. Chang et al. [14] proposed an elegant SVD-based watermarking scheme, but it has some weaknesses. Patra et al. [15] have reported an improved SVD-based scheme that has overcome the weaknesses of Chang et al.'s scheme.

2.1. Watermarking Scheme 1

Let A be a matrix of size $M \times N$ representing an image. The elements of A will have values between 0 and 255, for 8-bit representation of the pixels. Using singular value decomposition the matrix A can be decomposed into three matrices as follows:

$$A = UDV^T$$

$$= \begin{bmatrix} u_{11} & u_{12} & \dots & u_{1M} \\ u_{21} & u_{22} & \dots & u_{2M} \\ \dots & \dots & \dots & \dots \\ u_{M1} & u_{M2} & \dots & u_{MM} \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 & 0 & \dots & 0 \\ 0 & \lambda_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda_M \end{bmatrix} \begin{bmatrix} v_{11} & v_{21} & \dots & v_{N1} \\ v_{12} & v_{22} & \dots & v_{N2} \\ \dots & \dots & \dots & \dots \\ v_{1N} & v_{2N} & \dots & v_{NN} \end{bmatrix}, \quad (1)$$

where U ($M \times M$) and V ($N \times N$) represent the orthogonal matrices of A , and D ($M \times N$) (same dimension as A) represents a diagonal matrix. The eigen-vectors of AA^T make up the columns of U and the eigen-vectors of $A^T A$ are the columns of V . The diagonal elements of D represent square root of eigen-values of either $A^T A$ or AA^T , and these are arranged in descending order, i.e., $\lambda_1 > \lambda_2 > \lambda_3 > \dots$. The rank of A is defined as the number of non-zero diagonal elements of D .

The SVD-based watermarking scheme proposed by Chang et al. [14] uses a block-based SVD technique. The scheme is quite promising, however, the main weakness of this scheme is its reliance on the use of rank in selecting an image block

Fig. 1. Watermarking Scheme 1. The change in rank results in a shifted Panda in the extracted watermark: (a) original 16×16 watermark, (b) extracted 16×16 watermark, (c) difference between original and extracted watermarks.

for embedding watermark bits. This reliance causes the scheme to be less resistant to attacks, which alters the rank of the image blocks. The host image is a grey-scale image and the watermark is a binary image. First, the host image is divided into blocks of $n \times n$ pixels. A single watermark bit is embedded in a block. The blocks are chosen randomly using a pseudo-random number generator (PRNG) based on their rank. The blocks with higher ranks are selected first before those of lower ranks.

In order to embed a watermark bit in a block the following procedure is adopted. We first perform a SVD transformation on the selected block. Let c_1 and c_2 denote the second and the third elements (u_{21} and u_{31}) of the first column of U matrix, respectively. The embedding rules are as follows:

To embed a watermark bit '1,' the value of $c_1 - c_2$ should be positive and its magnitude is greater than a strength factor, s . If this condition is not satisfied, c_1 and c_2 are modified as c'_1 and c'_2 , respectively, and are given by

$$\begin{aligned} c'_1 &= a + s/2, \\ c'_2 &= a - s/2, \end{aligned} \quad (2)$$

where $a = (|c_1| + |c_2|)/2$.

To embed a watermark bit '0,' the value of $c_1 - c_2$ should be negative and its magnitude is greater than the strength factor, s . If this condition is not satisfied, c_1 and c_2 are respectively modified as c'_1 and c'_2 given by

$$\begin{aligned} c'_1 &= a - s/2, \\ c'_2 &= a + s/2. \end{aligned} \quad (3)$$

To reconstruct the watermarked block, an inverse SVD transformation is performed on the modified U matrix with the original D and V matrices. This watermarked block then replaces the original selected block in the host image. This embedding process is repeated until all the watermark bits have been embedded.

In this scheme, the selection of image blocks based on higher ranks would lower the distortion level of the watermarked image. However, the rank is not a reliable feature as it is not stable. The rank of the selected block could change after modifications are made to the elements c_1 and c_2 . Therefore, without any tampering to the watermarked image, the extracted watermark could be corrupted due to a change in rank of the block. Fig. 1 shows the corruption of the extracted watermark due to changes in rank. In general, when the strength factor increases, the likelihood of changing of the rank of a block increases. This leads to a higher level of corruption and distortion in the watermark and watermarked image, respectively.

The initial steps of the extraction procedure are similar to that of the embedding process up to and including the selection of the coefficients c_1 and c_2 . The value of $c_1 - c_2$ determines the value of the extracted watermark bit. A positive difference indicates that the watermark bit is a '1.' Whereas, a negative difference would imply that a watermark bit '0' is extracted.

2.2. Watermarking Scheme 2

The embedding procedure of the scheme proposed by Patra et al. [15] is an improved version of Scheme 1. The host image is divided into a number of super-blocks that is equal to the number of watermark bits. From each super-block, a sub-block is selected which is transformed via SVD to embed the watermark. Instead of embedding exclusively in the U matrix, the V matrix is also utilized. A counter is introduced to allow random selection of embedding the watermark bit in either U or V matrix to improve the security and robustness.

In addition, the coefficients (c_1 and c_2) are selected randomly from the first column of the U or V matrices using a PRNG. This flexibility gives an edge over the scheme proposed by Chang et al. [14], as malicious tampering cannot be targeted at the two modified coefficients due to their random selection. However, to minimize the distortion to the watermarked image, the position of c_2 must be consecutive to c_1 . Experiments show that the watermarked image quality reduces as the distance between the modified coefficients is increased. The modifications of c_1 and c_2 are similar to the procedure in Scheme 1. The reconstruction of the new block, re-placement of the block into the image, and extraction procedure are also similar to that of Scheme 1.

This scheme removes the reliance on rank and also improves security by using random selection of coefficients for embedding the watermark bits. The weakness of this scheme is that the robustness of the scheme is inversely proportional

to the watermarked image quality. A higher strength factor would increase the watermarked image to be resistant to attacks, but it also means a drop in image quality. On the other hand, too low a strength factor would reduce its robustness against attacks. Moreover, the concept of using a super-block in this case causes a sharp drop in the capacity of embedded watermark bits. It may be insufficient for a small-sized watermark to provide evidence of ownership of a document or an image.

3. Chinese remainder theorem

3.1. The CRT

The CRT can be compactly stated as follows. Let μ be a set of r integers given by $\mu = \{M_1, M_2, \dots, M_r\}$, such that M_i are pair-wise relatively prime. Let a set of r simultaneous congruences is given by

$$Z \equiv R_i \pmod{M_i}, \quad (4)$$

where R_i are called residues. The solution for the integer Z can be found as

$$Z \equiv \left(\sum_{i=1}^r R_i \frac{M}{M_i} K_i \right) \pmod{M}, \quad (5)$$

where $M = M_1 \cdot M_2 \cdot \dots \cdot M_r$ and K_i are determined from

$$K_i \frac{M}{M_i} \equiv 1 \pmod{M_i}. \quad (6)$$

Let us take a simple example with $r = 2$ to illustrate CRT. Let $M_1 = 6$, $M_2 = 11$, and $R_1 = 4$, $R_2 = 8$. That is, $Z \equiv 4 \pmod{6}$ and $Z \equiv 8 \pmod{11}$. Compute $M = M_1 M_2 = 66$. K_1 and K_2 are to be determined such that (6) is satisfied. That is, $(K_1 \frac{66}{6}) \equiv 1 \pmod{6}$ and $(K_2 \frac{66}{11}) \equiv 1 \pmod{11}$. We can see that for $K_1 = 5$ and $K_2 = 2$, these two equations are satisfied. Now Z is determined as $Z \equiv (4 \cdot \frac{66}{6} \cdot 5 + 8 \cdot \frac{66}{11} \cdot 2) \pmod{66} = 52$.

3.2. The inverse CRT

Given that $\mu = \{M_1, M_2, \dots, M_r\}$ and $M = M_1 \cdot M_2 \cdot \dots \cdot M_r$. The objective of the inverse CRT is to represent any integer Z , $\{0 < Z \leq M - 1\}$ by a set of integers $Z = \{R_1, R_2, \dots, R_r\}$. The R_i are obtained from the following congruences:

$$Z \equiv R_i \pmod{M_i}. \quad (7)$$

Let us take the previous example in which $M_1 = 6$ and $M_2 = 11$. Therefore, $M = M_1 M_2 = 66$. Let the given integer be $Z = 52$. Using (7), $52 \equiv R_1 \pmod{6}$ and $52 \equiv R_2 \pmod{11}$. Thus, we get $R_1 = 4$ and $R_2 = 8$. Therefore, Z can be represented as $Z = \{4, 8\}$. For detailed discussions on CRT, one can refer to any textbook on number theory or cryptography [22,23].

4. Proposed CRT-based watermarking scheme

The embedding and extraction procedure of the proposed scheme is based on CRT technique. This scheme attempts to provide improved security and minimal distortion to the host image. In addition, it needs minimal information during extraction phase and provides robustness to some severe attacks.

4.1. Embedding procedure

The process begins by dividing the host image into equal-sized blocks based on the number of watermark bits to be embedded. For example, to embed a 32×32 binary watermark (black and white) into a 256×256 host image, the host image is divided into 1024 blocks each of size 8×8 . Therefore, there would be one watermark bit embedded in each block. After dividing the host image into blocks, consider one block at a time to embed the watermark bits. The pixel intensity of the host image is represented by 8-bits. Therefore, the pixel intensity ranges from 0 to 255 (0 and 255 represent pure black and pure white, respectively). The embedding procedure is given by the following steps:

- Step 1. Select the pixel (with intensity X), to be embedded in a block, using a PRNG.
- Step 2. Convert the decimal value of X , which ranges from 0–255, into a binary form.
- Step 3. Consider the 6 least significant bits (LSBs) of X and convert it into a decimal value Z . The range of Z is 0–63.
- Step 4. Consider the 2 most significant bits (MSBs) of X and convert it into a decimal value Y , which can take the values 0, 64, 128 and 192.
- Step 5. Select the pair-wise co-prime numbers as $M_1 = 6$, $M_2 = 11$.
- Step 6. Find R_1 and R_2 for Z by applying the inverse CRT using (7).

Step 7. To embed bit '1,' the required condition is given by

$$R_1 \geq R_2. \quad (8)$$

If (8) is not satisfied, then Z is modified using the modification procedure, as explained below, until it is satisfied.

Step 8. To embed bit '0,' the required condition is:

$$R_1 < R_2. \quad (9)$$

If (9) is not satisfied, then Z is modified using the modification procedure, as explained below, until it is satisfied.

Step 9. After deciding on the values R_1 and R_2 , using CRT (5) combine them with M_1 and M_2 to get Z' .

Step 10. Combine the value of Y with Z' to get X' , the new watermarked pixel value.

Step 11. Reconstruct the block with the new watermarked pixel value X' .

Step 12. Repeat Steps 1–11 for all the blocks until all the watermark bits are embedded.

There were some considerations to be made for embedding a watermark bit. Firstly, we are using only the 6 LSBs and not the full 8 bits, because we do not want to modify the pixel values to a large extent, which can cause some visual distortion. Our focus in this scheme is to keep distortion minimal. Secondly, we have selected the pair-wise co-prime numbers M_1 and M_2 , as 6 and 11, respectively. According to CRT, the product of the pairwise coprime numbers should be greater than the possible range of numbers under consideration, which in our case is 0–63. Another reason behind choosing 6 and 11 instead of other numbers is that the maximum possible pixel intensity, 63 is close to 66. This allows minimum distortion to the watermarked pixel.

We have mentioned that to embed bits '1' and '0' some conditions are to be satisfied. If these are not fulfilled, the value of Z is to be systematically modified. This is carried as follows.

1) Modification procedure to embed bit '1':

First check whether the condition (8) is satisfied. If it is satisfied, then there is no need to modify the value of Z . Otherwise subtract 1 from Z . Going back to Step 6, check whether condition (8) is satisfied. If it is satisfied then select new value of Z . Otherwise, add 1 to Z , continue with Step 6 and check whether (8) is satisfied. If adding or subtracting 1 does not yield the expected result, then carry on subtracting or adding 1 to Z until (8) is satisfied. Thereafter, the modified values of R_1 and R_2 are used by CRT (5) to get Z' .

2) Modification procedure to embed '0':

In this case, the modification procedure is the same as that of bit '1' except that the condition to be checked is (9).

A flow-chart illustrating the above embedding procedure is shown in Fig. 2.

4.2. Extraction procedure

The extraction procedure is reverse of the embedding procedure. We need to know only the following information to extract the watermark from the watermarked image.

1. Watermarked image.
2. Size of the watermark.
3. Seed of the PRNG.
4. The pair-wise co-prime numbers M_1 and M_2 .

With the knowledge of PRNG, the pixel of the block in which watermark is embedded is selected and its pixel value Z is found out. Thereafter, using M_1 , M_2 and Z , R_1 and R_2 are determined using (7). After which, a comparison is made between R_1 and R_2 . If $R_1 \geq R_2$, bit '1' would be extracted, otherwise bit '0' would be extracted. These steps are repeated for every consecutive block to extract all the watermark bits.

5. Experimental results

In order to carry out the comparison between the proposed and the SVD-based techniques, few performance measures are defined below. The extent of tampering of the extracted watermark is computed using Tampered Assessment Function (TAF) [22]. Considering the size of the watermark as $m \times n$, the TAF in percentage is defined as

$$TAF = \frac{1}{mn} \left[\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} w(i, j) \oplus \bar{w}(i, j) \right] \times 100, \quad (10)$$

Fig. 2. Flow-chart to embed a watermark bit.

where, $w(i, j)$ and $\bar{w}(i, j)$ represent the original and extracted watermarks at position, (i, j) respectively, and $\oplus$ is an exclusive-OR operator. The acceptance level of TAF is 5% because, above this value, the extracted watermark will not be recognizable.

Peak Signal-to-Noise Ratio (PSNR) measures the quality between two images. Usually we would compare the modified signal against the original signal, i.e., in this case, the watermarked image against the original host image. The value of PSNR usually ranges from 20 dB (low quality) to 40 dB (high quality). Since the host images used for the experiments are in 8-bit gray-scale format, the peak value of the image is taken to be 255. The PSNR in dB is given by

$$PSNR = 10 \log_{10} \left[\frac{255^2}{\frac{1}{M} \frac{1}{N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [A(i, j) - \bar{A}(i, j)]^2} \right], \quad (11)$$

where, A represents the host image, $\bar{A}$ represents the watermarked image and M and N represent the dimensions of the two images.

In this study we carry out performance comparison among the three schemes considering the following performance criteria:

1. Computational complexity of the embedding and extracting procedures.
2. Quality of the watermarked images.
3. Robustness of the schemes to different attacks.
4. Further increase in embedding capacity.

Fig. 3. The three host images (256×256): (a) Lenna, (b) Baboon, (c) Airplane, and (d) the watermark image, Panda (64×64).

Fig. 4. Comparison of embedding and extracting times for the three schemes: (a) embedding time, (b) extraction time.

5.1. Computational complexity

The computational time for embedding and extraction is an important performance measure, especially when the watermarking is to be carried out for online applications, e.g., video or audio broadcasting. Several experiments were conducted to evaluate performance of the proposed scheme against the two SVD-based schemes. The experiments were carried out in a laptop PC with Intel Pentium M processor, 1.70 GHz clock and 512 MB RAM. Three benchmark gray-level images of 256×256 pixels of Lenna, Baboon and Airplane were used as host images, as shown in Fig. 3. A black and white (binary) image of Panda was used as the watermark. Several watermark dimensions were used in the simulations, i.e., 32×32 , 32×64 , 64×64 and 128×64 . The results are based on Lenna (host image, 256×256) watermarked with Panda (watermark, 32×32), unless otherwise stated. We have observed that the results of simulations using the other two host images (Baboon and Airplane) were similar to that of Lenna.

We compare the embedding and extraction time of the proposed scheme against Schemes 1 and 2. Ten simulation runs were conducted for each scheme to determine the average timing for each scheme and are plotted in Fig. 4. The host images were watermarked with Panda image (32×32).

From Fig. 4 one can see that the proposed scheme is able to embed and extract the watermark in much less time than Schemes 1 and 2. On averaging over the three host images, the embedding time for Scheme 1, Scheme 2 and proposed CRT-based scheme were found to be 250, 130 and 40 ms, respectively. The proposed scheme is faster because only simple CRT calculations are required for embedding, which makes up the bulk of the embedding time. The difference in timings between Schemes 1 and 2 is due to the calculation of ranks of the individual blocks and selection of blocks to embed the watermark bits. Furthermore, it can also be seen that the time taken to select blocks based on rank is image-dependent that gives rise to significant differences in timing. However, in our proposed scheme, the embedding time is found to be independent of the host image. The extraction time in the proposed scheme (as shown in Fig. 4(b)) is also reduced to a large extent, because only CRT calculations are needed during extraction phase. The average extraction time for Scheme 1, Scheme 2 and proposed scheme was observed to be 190, 90 and 20 ms, respectively. It is also noticed that unlike the two SVD-based schemes, the extraction time in our proposed scheme does not depend on the host image. Scheme 2 is faster than Scheme 1 because of absence of rank calculation and selection of blocks based on rank.

The computational advantage of the proposed scheme is derived from the fact that CRT involves only modular operations which are computationally efficient compared to SVD. In the SVD-based Schemes 1 and 2, the basic operations involved in the embedding phase are given by: (i) given a matrix A , generate the three matrices, U , V and D , (ii) manipulate some elements of U or V matrix, and (iii) obtain the matrix $\hat{A}$ through SVD using modified U , V and D . In our proposed scheme, the basic operations in the embedding stage are given by: (i) given an integer Z , using CRT determine the residues R_1

Fig. 5. Quality of watermarked image in PSNR for different host images.

and R_2 , (ii) check the embedding conditions, and (iii) modify Z until embedding conditions are satisfied. We simulated these operations in an Intel Duo P8600-based CPU with 2.40 GHz clock and 4 GB RAM using JAVA programming language. The average computation time for one run of the SVD and CRT based basic operations were found to be 37 ms and 92 ns, respectively. This shows that the CRT-based computations are much faster than SVD computations. The relative timings shown in Fig. 4 are much higher because they were based on a different PC specification and are meant for complete embedding and extraction phases.

5.2. Quality of watermarked images

The quality of the watermarked images used to embed the watermark with respect to the different schemes is investigated here. Fig. 5 shows the quality of the watermarked images based on PSNR for the different host images. In Schemes 1 and 2, a strength factor, $\alpha = 0.02$ was used for embedding. The performance difference between Schemes 1 and 2 is not significant. Note that Scheme 1 utilizes the rank property of the block matrices by giving preference to higher ranked blocks during the embedding procedure. However, it does not seem to have a clear advantage in quality of the watermarked image when compared to Scheme 2. It can be seen that our proposed scheme is superior in terms of PSNR than the other two schemes for different host images. The PSNR of the watermarked image in the CRT-based scheme is about 60 dB, whereas in Schemes 1 and 2 it remains between 30 to 40 dB.

In order to have a visual inspection, we magnified the Lenna image that was watermarked using the three schemes. The magnified images along with the original image are shown in Fig. 6. One can notice by close visual inspection that the resemblance of images between the original (top left) and the watermarked with the proposed scheme (bottom right) is higher than that with the other two schemes. This provides the evidence that least distortion occurs to the host image that is watermarked with the CRT-based scheme.

5.3. Robustness against attacks

In this section, we compare the proposed scheme against Schemes 1 and 2 in their ability to withstand different types of attacks. The watermarked image was subjected to different attacks, such as, addition of noise and tampering, before extracting the watermark. The quality of the extracted watermark is determined by their TAF value (10). A lower TAF value would indicate that the extracted watermark is more similar to the original watermark.

Several image manipulation techniques were used to distort the watermarked images. These techniques are: (i) Cropping of a block size of 32×32 at the upper left corner of the image, (ii) tampering 25% of the pixels with a strength factor of 25, (iii) adding noise to the entire watermarked image with a 20% distortion rate, (iv) JPEG compression with a value of 0.75, and (v) brightening the watermarked image to 140%.

Fig. 7 shows the TAF of the extracted watermarks after the watermarked images are subjected to noise attack. Note that this figure is based on host image Lenna (256×256), watermark image Panda (32×32) and block size $= 8 \times 8$. A strength factor, $s = 0.02$ was used in Schemes 1 and 2. It can be seen that the TAF performance of Schemes 1 and 2 is similar. But the proposed scheme outperforms the other two schemes, especially when the additive noise is between 15 to 30 dB. For example, with an additive noise of 17 dB, TAF for the proposed scheme is only 4%, whereas for Schemes 1 and 2, it is 31% and 29%, respectively.

The performance comparison in terms of TAF for the cropping and tampering attacks is shown in Fig. 8. The host Lenna image was watermarked with Panda image (32×32) and a block size of 8×8 was used. It can be seen that all the three schemes performs similarly for tampering attack. However for the cropping attack, the proposed scheme does not perform as well as Scheme 2, but performs better than Scheme 1. The extracted watermark based on Scheme 1 has high

Fig. 6. Magnified images: top left – original host image; top right – watermarked with Scheme 1, bottom left – watermarked with Scheme 2, bottom right – watermarked with proposed scheme.

Fig. 7. Quality of extracted watermark due to noise addition attack.

TAF percentage. This means that the extracted watermark is not recognizable and thus unable to prove ownership of the image. This is probably due to the usage of ranks in the selection of a block for embedding the watermark bit.

The experimental results for the JPEG compression, brightening and sharpening attacks showed that the proposed scheme is not as robust as Scheme 2, as the TAF is more than 30% which voids the watermark. Scheme 1 is quite robust to sharpening attack but not so much for JPEG compression and brightening attacks as compared to Scheme 2. The results for blurring and scaling down attacks were omitted as all the schemes were unable to extract a recognizable watermark. The TAF is found to be more than 30% which voids the watermark. All these tests were conducted on the other two host images and similar results were observed.

Some extracted watermark images for different attacks are shown in Fig. 9. It can be seen that for the proposed scheme, there is a significant improvement in the quality of extracted watermarks from the watermarked images subjected to noise addition. There is also noticeable improvement for cropping attack compared to Scheme 1. The TAF of the extracted watermarks under different attacks to the watermarked Lenna image are shown in Table 1 in which Scheme 1, Scheme 2 and the proposed scheme are denoted by (a), (b) and (c), respectively. It can be seen that the proposed scheme outperforms other

Fig. 8. Quality of extracted watermark after cropping and tampering attacks.

Fig. 9. Watermarks extracted from the attacked watermarked Lenna image.

Table 1

TAF of the watermarks extracted from the attacked watermarked images: (a) Scheme 1, (b) Scheme 2, (c) proposed scheme.

Host images	Attacks														
	Cropping			Tampering			Addition of noise			JPEG compression			Brightening		
	(a)	(b)	(c)	(a)	(b)	(c)	(a)	(b)	(c)	(a)	(b)	(c)	(a)	(b)	(c)
Airplane	40.63	0	1.56	0.20	0.20	0.29	13.57	13.38	2.83	35.45	0.88	40.72	40.43	17.68	32.03
Baboon	40.63	0	1.56	0.20	0	0.10	19.63	18.95	2.34	1.37	4.59	42.87	35.74	1.46	42.48
Lenna	40.63	0	1.56	0.10	0.10	0.10	23.93	22.46	1.86	32.23	12.60	43.65	30.18	2.05	48.54

two schemes against noise attack. For cropping and tampering attacks, both the proposed scheme and Scheme 2 perform much better than Scheme 1.

However, the proposed scheme is not as robust as Scheme 2 against JPEG compression and brightening attacks. The reason for the unsatisfactory performance against JPEG compression is probably due the fact that JPEG compression is based on discrete cosine transform (DCT), where as in the proposed scheme, watermarking is carried out in spatial domain. Therefore, we believe that if the CRT-based watermarking scheme is carried out in DCT domain, performance against JPEG compression can be improved.

5.4. Increase of watermark capacity

The proposed scheme utilizes all the blocks in the host image to embed the watermark bits. The watermark embedding capacity in the host image can be doubled by embedding two bits per block instead of one. This is done by embedding the second bit by selecting the pixel just below the first embedded pixel. We have seen that by doing so the quality of the watermarked image drops about 2–4 dB when all other conditions remain the same. This drop in image quality is not significant as differences in watermarked images based on the original and modified proposed scheme are not noticeable to the human eye. Fig. 10 shows the results of this scheme based on host image Lenna (256×256), watermark image Panda (64×32), block size = 8×8 . A strength factor, $s = 0.02$, was used for Schemes 1 and 2. It may be observed that the proposed scheme maintains its superiority in PSNR compared with other two schemes when the watermark capacity is doubled. In this case, the quality of the extracted watermark under addition of noise is similar to that of Fig. 7. In case of other attacks (cropping and tampering) the performance is similar to that of Fig. 8, but with a slight deterioration. Despite

Fig. 10. Quality of watermarked image (PSNR) for different host images after doubling of watermarking capacity in the proposed scheme.

having doubled the amount of watermark bits embedded, the modified proposed scheme maintains its superiority in being robust in handling noise addition, cropping and tampering attacks.

6. Conclusion

In this paper we have proposed a new approach based on CRT for watermarking of images for authentication. This technique can also be applied to other multimedia contents, such as, documents, audio and video. The use of CRT provides advantage in terms of improved security and low computational complexity. In this scheme only a few information are needed for extraction of watermark. We have compared its performance with two other recently reported SVD-based watermarking schemes [14,15] and shown that the proposed scheme outperforms the other two in terms of distortion in the watermarked image and some of major attacks. Especially, the proposed technique exhibits strong resistance to the addition of noise attack. The time required for embedding and extraction of watermark in the proposed scheme is much less compared to that of the two SVD-based schemes. The proposed scheme can increase the embedding capacity in the host image while maintaining imperceptibility and robustness against attacks. However, the proposed scheme is not robust against JPEG compression and brightening attacks. We believe that by implementing the proposed scheme in DCT domain, these deficiencies can be well tackled.

Acknowledgments

The authors would like to offer their sincere thanks to the anonymous reviewers whose positive and constrictive comments and suggestions helped to enhance the quality of the paper to a great extent.

References

- [1] W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, *IBM Syst. J.* 35 (3–4) (1996) 313–336.
- [2] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, *IEEE Trans. Image Process.* 6 (12) (1997) 1673–1687.
- [3] I.J. Cox, M.L. Miller, A.L. McKellips, Watermarking as communication with side information, *Proc. IEEE* 87 (7) (1999) 1127–1141.
- [4] P.W. Wong, N. Memon, Secret and public key image watermarking schemes for image authentication and ownership verification, *IEEE Trans. Image Process.* 10 (10) (2001) 1593–1601.
- [5] T.H. Chen, D.S. Tsai, Owner–customer right protection mechanism using a watermarking scheme and a watermarking protocol, *Pattern Recognition* 39 (8) (2006) 1530–1541.
- [6] C.Y. Lin, S.F. Chang, A robust image authentication method distinguishing JPEG compression from malicious manipulation, *IEEE Trans. Circ. Syst. Video Technol.* 11 (2) (2001) 153–168.
- [7] C.T. Hsu, J.L. Wu, Hidden digital watermarks in images, *IEEE Trans. Image Process.* 8 (1) (1999) 58–68.
- [8] P. Loo, N. Kingsbury, Watermark detection based on the properties of error control codes, *IEE Proc. Vis. Image Signal Process.* 150 (2) (2003) 115–121.
- [9] T.V. Nguyen, J.C. Patra, A simple ICA-based watermarking scheme, *Digit. Signal Process.* 18 (2008) 762–776.
- [10] R. Liu, T. Tan, An SVD-based watermarking scheme for protecting rightful ownership, *IEEE Trans. Multimed.* 4 (1) (2002) 121–128.
- [11] J.M. Shieh, D.C. Lou, M.C. Chang, A semi-blind digital watermarking scheme based on singular value decomposition, *Comput. Stand. Interf.* 28 (4) (2006) 428–440.
- [12] S. Lee, D. Jang, C.D. Yoo, An SVD-based watermarking method for image content authentication with improved security, in: *Proc. IEEE Int. Conference on Acoustics, Speech, and Signal Processing*, vol. 2, IEEE, March 2005, pp. 525–528.
- [13] K.L. Chung, W.N. Yang, Y.H. Huang, S.T. Wu, Y.C. Hsu, On SVD-based watermarking algorithm, *Appl. Math. Comput.* 188 (1) (2007) 54–57.
- [14] C.-C. Chang, P. Tsai, C.-C. Lin, SVD-based digital image watermarking scheme, *Pattern Recognition Lett.* 26 (2005) 1577–1586.
- [15] J.C. Patra, W. Soh, E.L. Ang, P.K. Meher, An improved SVD-based watermarking technique for image and document authentication, in: *Proc. IEEE Asia Pacific Conference on Circuits and Systems*, Singapore, December 2006, pp. 1984–1987.
- [16] T.-S. Chen, Y.-F. Chung, Hierarchical access control based on Chinese remainder theorem, *Comput. Secur.* 2 (6) (2002) 565–570.
- [17] C.-C. Chang, Y.-P. Hsieh, C.-H. Lin, Sharing secrets in stego images with authentication, *Pattern Recognition* 41 (2008) 3130–3137.
- [18] S. Myung, K. Yang, A combining method of quasi-cyclic LDPC codes by Chinese remainder theorem, *IEEE Comm. Lett.* 9 (9) (2005) 823–825.

- [19] E. Al-Radadi, P. Siy, RNS sign detector based on Chinese remainder theorem II (CRT II), *Comput. Math. Appl.* 46 (2003) 1559–1570.
- [20] C.-C. Chang, J.-S. Lee, Robust t -out-of- n oblivious transfer mechanism based on CRT, *J. Netw. Comput. Appl.* 32 (1) (2009) 226–235.
- [21] J.C. Patra, A. Karthik, P.K. Meher, C. Bornand, Robust CRT-based watermarking technique for authentication of image and document, in: *Proc. IEEE Int. Conf. Systems, Man, and Cybernetics (SMC 2008)*, Singapore, October 2008, pp. 3250–3255.
- [22] B. Schneier, *Applied Cryptography*, 2nd edition, Wiley, New York, 1996.
- [23] D.R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, FL, 1995.

Jagdish C. Patra received B.Sc. (Engg.) and M.Sc. (Engg.) degrees, both in electronics & telecommunication engineering, from Sambalpur University, India, in 1978 and 1989, respectively. He obtained Ph.D. degree in electronics & communication engineering from Indian Institute of Technology, Kharagpur, India, in 1997. After Bachelor's degree, he worked in various R&D, teaching and government organizations for about eight years. In 1987, he joined Regional Engineering College, Rourkela, India, as a Lecturer, where he was promoted to Assistant Professor in 1990. In April 1999, he visited Technical University, Delft, Netherlands, as a Guest Teacher (Gastdocent).

Since 2001, he is an Assistant Professor in the School of Computer Engineering, Nanyang Technological University, Singapore. His research interests include intelligent information processing using neural networks in the areas of data security, sensor networks, image processing and bioinformatics. In these areas, he has over 100 research publications in international journals of repute and top international conferences. He is a Member of IEEE (USA) and Life Member of Institution of Engineers (India).

A. Karthik obtained Bachelor of Engineering (Computer Engineering) degree with a Minor in Business from Nanyang Technological University, Singapore in 2008. After completion of Bachelor's degree, he is currently working in IBM, Singapore as a Consultant. He has done his Internship with Citibank, Singapore as a Web Software Engineer in 2007. He has completed his National Service with the Singapore Armed Forces in 2004. His research interests include development of novel techniques for digital watermarking, data hiding and multimedia applications. He has other interests and hobbies which include playing cricket, soccer and badminton, listening to music and watching movies.

Cédric Bornand graduated from the Swiss Federal Institute of Technology, Lausanne (EPFL), in 1988. Currently, he is a full professor at the University of Applied Sciences, HEIG-VD, Switzerland, and manages a research group in the field of embedded sensors. Over the last twenty years his team has carried out research in various aspects of sensors applications, ranging from mechanical measurements to traffic regulation, developing effective online algorithms as well as hardware implementations. Cédric Bornand focused his activities on multimodal systems and biomedical applications, with a strong effort in the integration of algorithms on various DSP solutions.