High Payload Watermarking using Residue Number System

Shubhendu Banerjee
Dept. of CSE, Narula Institute of Technology, Kolkata, West Bengal, India,
shankushubhendu@gmail.com

Sayan Chakraborty, Nilanjan Dey
Dept. of CSE, Bengal College of Engineering & Technology, Durgapur, West Bengal, India,
Email: sayan.cb@gmail.com, neelanjan.dey@gmail.com

Arijit Kumar Pal
CMC Limited, India,
arijit1421@gmail.com,

Ruben Ray
Dept. of IT, Government College of Engineering and Leather Technology, Kolkata, West Bengal, India,
ruben.ray@gmail.com

Abstract—Information hiding or data hiding, also known as watermarking, has become a part and parcel of covert communication and copyright protection. Maximizing watermark payload is a major challenge for watermark researchers. To overcome this issue, we have proposed a new color image watermarking technique, using residue number system (RNS). RNS refers to a large integer using a set of smaller integers which relies on the Chinese remainder theorem of modular arithmetic for its operation. The proposed method takes pixel values from three watermark images and embeds them into the main cover image. Experimental results presented in this paper shows that the watermark can be successfully embedded and extracted from an image, without distorting the original image using the proposed technique. The high peak signal to noise ratio (PSNR) and payload values claims the robustness of the proposed method.

Index Term—Watermarking, Payload, Residue Number System, Chinese Remainder Theorem, PSNR.

I. INTRODUCTION

Hiding any message within an image, signal or video is known as watermarking [1]. To hide the message, an image is used as a cover, which is intended for transfer. Digital watermarking has become an integral part in various applications. Watermarking [2, 3, 4] is mainly used for security purpose. Imperceptibility and robustness are two main features of a good watermark [5,6]. Robust watermarking [7, 8, 9] means, when an image is less damaged after retrieving. If the quality of the watermarked [10, 11, 12] image is seriously affected after embedding, then the watermarked image can be identified easily. The property of less degradation of an image is referred to as imperceptibility [13, 14, 15]. The secret message is embedded as an invisible mark [16,17] and recovered back after the extraction of watermark. The traditional watermarking [18, 19, 20] techniques can be divided into two categories: spatial domain information hiding and transform domain (such as the DCT transform domain, the wavelet transform domain, etc.). In spatial domain information hiding, most watermarking [21, 22] methods embed the information directly to the original image. If some valuable information which was required during embedding watermark [23, 24] is provided to the user, then it should be non-blind watermarking [25, 26, 27]. The properties are the same as watermarking scheme. The watermark can be easily embedded [28, 29] and retrieved by the users. Payload means the amount of data which requires to be watermarked. High payload in watermark [30, 31] refers to the method that can hide large amount of data. The chief factors influencing payload are size of an image or data, the embedding intensity, image roughness, visual sensitivity etc. High payload and better watermark [32, 33] leads to perceptual invisibility.

In 1999, Johnson [1] et al. proposed a method of recovering watermark from images after it suffered some type of attacks. Some watermarking methods which has suffered from attacks such that the hidden secret information cannot be recovered, was included in this work. In 2001, Lu [2] et al. proposed a watermarking scheme for the purpose of image authentication and protection. Two watermarks are embedded using quantization of wavelet coefficients of the host image and they are extracted without accessing the original image. In 2004, Wang [3] et al. proposed an RNS application for digital image processing. In this paper, a study on the RNS (residue number system) application in digital image processing was done and a RNS image coding scheme that offers high-speed and low-power VLSI implementation for secure image processing was proposed.
In 2006, Castillo [4] et al. proposed an RNS-based watermarking for IP cores. In this technique, electronic digital signature embedding using RNS-based designs was used to protect the author rights of IP cores. In 2008, Zhao [5] et al. proposed a reversible watermarking scheme. In this paper, a pair of pixel is considered and a certain value is added to one and subtracted from the other to balance distortion. A series of experiments established the effectiveness of this method. In 2009, Kumari [6] et al. proposed a watermarking technique for gray level images. The watermark is inserted using LSB. The gray value of the image does not change successively and later a secret message is inserted in the image using those gray values. In 2010, Wu [7] et al. presented a paper on fixed point and floating point data. In this paper, watermarked image [8, 9, 10] is exploited to get the actual recovery of the original value with the smallest error and then a pseudorandom sequence was added to the watermarked [11, 12] object for security purpose.

Methodology is described in section 2. Section 3 illustrates the proposed method. Proposed method is further explained in detail in section 4. Simulation results is shown in section 5 and also analysis of those obtained results are done in the same section. Paper concludes in section 6.

II. METHODOLOGY
A. Residue Number System (RNS)

The residue number system is a non-weighted number system that has a certain advantage over the weighted number systems. RNS arithmetic is basically carry free and in the case of multiplication the need for partial products is eliminated.

In RNS representation of a number takes the form of N tuple of (x, x2, x3, ….xn). Here xi=X modulo mi, which is the i-th residue digit and mi is the i-th modulas and all mi are mutually prime numbers. Note that for maximum representation efficiency it is imperative that all the moduli are co-prime; that is no modulas may have a common factor with any other. The number of distinct values that can be represented, is called Dynamic range, M, where

\[ M = \prod_{i=0}^{N} m_i \text{ and } X \leq M \]  (1)

For signed RNS any integer in (-M/2, M/2), has a unique RNS. N tuple representation where x=X modulo mi if X > 0, and (M-[X]) mod m, otherwise.

Suppose there are two numbers A and B and after performing arithmetic operations a result is obtained which is denoted by C.

Now

\[ (A \ mod \ m1 \ m2 \ m3) = (a1 \ a2 \ a3) \]  (2)

\[ (B \ mod \ m1 \ m2 \ m3) = (b1 \ b2 \ b3) \]  (3)

\[ (C \ mod \ m1 \ m2 \ m3) = (c1 \ c2 \ c3) \]  (4)

o represents arithmetic operations i.e. addition, subtraction, multiplication.

Now,

\[ (A \ o \ B) = C \]  (5)

This implies,

\[ ((a1 \ o \ b1) \ modulo \ (m1 \ m2 \ m3) = (c1 \ o \ c2) \]  (6)

Suppose, A=7, B=3, m1=2, m2=3, m3=5; 7(1|1|2) + 3(1|0|3)=10(2 modulo 2| 1 modulo 3| 5 modulo 5)=10(0|1|0)

\[ X \ mod \ (m1 \ m2 \ m3) = (x1 \ x2 \ .... \ xn) \]  (6)

\[ Y \ mod \ (m1 \ m2 \ m3) = (y1 \ y2 \ .... \ yn) \]  (7)

\[ Z = X \ o \ Y \]  (8)

Here, o can represent addition, subtraction or multiplication.

\[ Z \ mod \ (m1 \ m2 \ m3) = (z1 \ z2 \ .... \ zn) \]  (9)

\[ =(X_1 \ o \ Y_1) \ mod \ p_1 , (X_2 \ o \ Y_2) \ mod \ p_2 , .... (X_n \ o \ Y_n) \ mod \ p_L \]

III. PROPOSED METHOD
A. Embedding Watermark within an image

Step 1. Color image is converted into 3 gray planes (Red, Blue and Green).

Step 2. Size of the image is calculated.

Step 3. Three binary images (same size of the color image) are taken as a watermark.

Step 4. Residue number system (RNS) [moduli of 3, 2 and 7 respectively] is applied on the first pixel value of the blue plane (gray).

Step 5. The very first bit is taken from each of the watermark image and the generated three bits are clubbed and converted into corresponding decimal number.

Step 6. RNS [mod of 3, 2 and 7 respectively] is applied on the generated decimal number.

Step 7. RNS addition is performed between the moduli results of the three numbers generated from step 4 and 6.

Step 8. The resultant three numbers are placed respectively to generate a single decimal number (Z) of length three (from the left the first digit or first & second both digits can be zero) for using the Step 9.

Step 9. The above produced decimal number Z is divided by 9 such that the quotient is y and the single digit remainder is x.

Step 10. x and y is clubbed together (yx) to give the watermarked pixel.

Step 11. Step 4 to 10 is applied for all the pixels of the blue plane of the color image and 3 watermark images to generate the watermarked image.
Step 12. The modified blue plane, red plane and green plane is combined to generate the color watermarked image.

B. Extraction of Watermark from Watermarked image

Step 1. Color watermarked image is again decomposed into three planes.

Step 2. The very first decimal number (yx) [where x is single digit] of the blue plane is expressed as the eqn. \( yx = 9^x y + x \).

Step 3. The resultant of \( 9^x y + x \) is separated into three individual digits (if the result is two digits then 1st digit is zero and if the result is one digit then both 1st and 2nd digits are zero).

Step 4. Chinese remainder theorem is applied to get back the original by taking moduli of 3, 2 and 7 for the respective three digits.

Step 5. Modulo results for 3, 2 and 7 (mutually prime) is summed up.

Step 6. The L.C.M. of 3, 2 and 7 i.e., 42 is added or subtracted from the generated sum repeatedly to find out the closest value of the first blue plane pixel.

Step 7. The first pixel value of the blue plane is subtracted from the generated closest value.

Step 8. The result is converted into binary number system i.e. three watermark bits.

Step 9. Step 2 to 8 is applied for all pixels of the whole watermarked image to retrieve the three watermark images.

IV. EXPLANATION OF THE PROPOSED METHOD

Let us consider that the first pixel (gray value) of the cover image is 255 and the first binary bits of the three watermarks [8, 9, 10] are 1, 0, 1 respectively as shown in the Fig. 1. The corresponding decimal number of 3 binary bits is 5. In the watermark embedding process, the Residue Number System (RNS) [Moduli of 3, 2 and 7 respectively] is applied on 255 and 5 to generate the following results:

\[ 255 \mod 3 = 0 \]
\[ 5 \mod 3 = 2 \]
\[ 255 \mod 2 = 1 \]
\[ 5 \mod 2 = 1 \]
\[ 255 \mod 7 = 3 \]
\[ 5 \mod 7 = 5 \]

The result of RNS addition will be as follows:

\[ (0 + 2) \mod 3, (1 + 1) \mod 2, (3 + 5) \mod 7 \]

which returns 2, 0, 1. 2, 0, 1 are clubbed together to generate a single decimal number 201 of length three digits.
If the generated single decimal number is 2 digit or single digit number e.g. 21 or 1 then we have to add an extra single 0 or two zeros in front of the digit to make it a number whose length is three e.g. 21 or 1 will consider as 021 and 001]. 201 is divided by 9 to generate the quotient 22 and the remainder 3. Then 22 and 3 are clubbed together (223) results, the watermarked pixel.

As an extraction [12, 13, 14] mechanism, 22 and 9 is multiplied and added with 3. The generated result (201) is split into 3 single digit numbers (2, 0, 1), i.e.-

\[\begin{align*}
201 \div 9 &= 22 \text{ remainder } 3 \\
22 \times 9 + 3 &= 201
\end{align*}\]

Chinese Remainder Theorem is applied by taking 2 for moduli 3, 0 for moduli 2, 1 for moduli 7.

- For mod 3: 2 and 7 are mutually prime. So the L.C.M. is 14 (2 x 7).
- For mod 2: 3 and 7 which were also mutually prime. So the L.C.M. is 21 (3 x 7).
- For mod 7: 2 and 3 are mutually prime and the L.C.M. of 2 and 3 is 6 (2 x 3).

Finally,

\[\begin{align*}
21 \mod 2 &= 1 \\
42 \mod 2 &= 0
\end{align*}\]

Hence, 21 will not be considered as a value.

\[\begin{align*}
21 \times 2 &= 42 \\
42 \mod 2 &= 0
\end{align*}\]

Thus, 42 will be considered for feather processing.

By subtracting 255 from 260, 5 is obtained. The binary representation of 5 is 101. Therefore the very first bit for each of the recovered watermark [15, 16, 17] image is 1, 0 and 1 respectively. The whole process is repeated for all other gray values with the help of watermark [18, 19] image bits of the corresponding positions. During extraction [20, 21, 22] process the recovery of watermark [23, 24, 25] requires the original gray value of the cover image blue plane. Hence, this proposed watermarking [26, 27, 28] is non-blind and lossless.

V. RESULTS AND DISCUSSION

MATLAB 7.0.1 Software is extensively used for the study of RNS based multiple image embedding technique. Concerned results are shown in Fig. 2 and Fig. 3.

![Fig. 2](image-url)

Fig. 2. (a) Lena cover image, (b) Baboon cover image, (c) Pepper cover image (d) Zelda cover image (e) Lena watermarked image (f) Baboon watermarked image (g) Pepper watermarked image (h) Zelda watermarked image.
Table 1 reports high PSNR and high correlation values obtained from current multiple image hiding technique [12, 13, 14]. To our knowledge, substantial amount of work has not been done in the domain of multiple image embedding. In 2013, Dey et al. proposed a method of multiple hospital logo embedding in retinal images using DWT-DCT-SVD [16] based technique. Considering the scaling factors \((k_1, k_2, k_3)=1\) the following results are obtained (Table 2). The comparative result clearly shows the efficacy and robustness of our proposed RNS based technique.

<table>
<thead>
<tr>
<th>Image</th>
<th>Size</th>
<th>PSNR</th>
<th>Normal Correlation between WM1 &amp; Recovered WM1</th>
<th>Normal Correlation between WM2 &amp; Recovered WM2</th>
<th>Normal Correlation between WM3 &amp; Recovered WM3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>512x512</td>
<td>30.1193</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Baboon</td>
<td></td>
<td>27.9376</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peeper</td>
<td></td>
<td>27.3506</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zelda</td>
<td></td>
<td>28.3780</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Image</th>
<th>Size</th>
<th>PSNR</th>
<th>Normal Correlation between WM1 &amp; Recovered WM1</th>
<th>Normal Correlation between WM2 &amp; Recovered WM2</th>
<th>Normal Correlation between WM3 &amp; Recovered WM3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>512x512</td>
<td>28.1686</td>
<td>0.9810</td>
<td>0.9495</td>
<td>0.9590</td>
</tr>
<tr>
<td>Baboon</td>
<td></td>
<td>27.8329</td>
<td>0.9841</td>
<td>0.9473</td>
<td>0.9669</td>
</tr>
<tr>
<td>Peeper</td>
<td></td>
<td>27.3158</td>
<td>0.9799</td>
<td>0.9505</td>
<td>0.9622</td>
</tr>
<tr>
<td>Zelda</td>
<td></td>
<td>27.9759</td>
<td>0.9799</td>
<td>0.9480</td>
<td>0.9608</td>
</tr>
</tbody>
</table>

Fig. 4 and Fig. 5 and Table 3 illustrate the effect of common attacks (effect of noise, rotation and flip) on the cover image. The obtained results show that RNS based technique is significantly robust and quiet encouraging. Table 1 also shows correlation between watermark and recovered watermark became 1, which ultimately denotes that our method is robust. Also, Table 2 shows other watermarking techniques’ results are poor compared to our method as the correlation obtained in those techniques are lesser than one.
Fig. 4. (a) Original image (b) 90° Rotated Image (c) 180° Rotated Image (d) Flipped image (e) Watermarked image (f) Watermarked 90° rotated Image (g) 180° Watermarked rotated image (h) Watermarked flipped image

Fig. 5. (a) Cover image with 5% Noise, (b) Cover image with 10% Noise, (c) Cover image with 30% Noise, (d) Cover image with 50% Noise, (e) Watermarked image with 5% Noise, (f) Watermarked image with 10% Noise, (g) Watermarked image with 30% Noise, (h) Watermarked image with 50% Noise

Table 3. Effect of Rotation, flip and noise.

<table>
<thead>
<tr>
<th>Image</th>
<th>Degree</th>
<th>PSNR</th>
<th>% of Salt pepper Noise</th>
<th>PSNR (After the effect of Noise)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>90°</td>
<td>30.1151</td>
<td>5</td>
<td>29.7026</td>
</tr>
<tr>
<td></td>
<td>180°</td>
<td>30.0903</td>
<td>10</td>
<td>29.3388</td>
</tr>
<tr>
<td></td>
<td>Flipped</td>
<td>30.0629</td>
<td>50</td>
<td>28.2708</td>
</tr>
</tbody>
</table>

VI. CONCLUSION

In this present work, we can embed 3 watermark images in a single image. Hence, the payload in this algorithm is extremely high. The watermarks are embedded in cover image and there was no distortion. Moreover, noise was mixed to establish much better comparison among the cover image and the watermarked image. The obtained values of correlation and PSNR are very much encouraging regarding the faithfulness of the reconstruction of the image. We have compared RNS technique with DWT-DCT-SVD based multiple image hiding technique. The obtained high PSNR value from our proposed RNS based multiple image embedding technique compared to the previous DWT-DCT-SVD based multiple image watermarking schema establishes the robustness of our proposed method.

REFERENCES


Authors’ Profiles

Shubhendu Banerjee, is currently working as Assistant Professor in the department of Computer Science & Engineering at Narula Institute of Technology, Kolkata, West Bengal, India. He has 1 publication in International conference proceedings. His research interest includes image and signal processing.

Sayan Chakraborty, is currently working as an Asst. Professor in Bengal College of Engg. & Tech, Durgapur, India. He has around 20 research papers in various international journals and conferences. Image processing and meta-heuristics is his research domain.

Nilanjan Dey, is a scholar of ETCE department, Jadavpur University, Kolkata, India. He is Visiting Scientist with Global Biomedical Technologies Inc., CA, USA. He is currently Asst. Professor in Bengal College of Engineering & Technology, West Bengal, India. He has more than 80 research papers in various national & international journals and conferences.

Arijit Pal, is Trainee, IT Engineer, in CMC limited, India. He completed his B.Tech from JIS College of Engg. in 2014 in Dept. of CSE. He has around 10 research papers in various international journals and conferences.

Ruben Ray is an assistant professor of Department of IT, Government College of Engineering and Leather Technology, Kolkata, India. His research area includes Sensor networking and remote sensing.

How to cite this paper: Shubhendu Banerjee, Sayan Chakraborty, Nilanjan Dey, Arijit Kumar Pal, Ruben Ray,”High Payload Watermarking using Residue Number System”, IJIGSP, vol.7, no.3, pp.1-8, 2015.DOI: 10.5815/ijigsp.2015.03.01