ParQuoSCI: Pseudorandom Partial Quotient Sequences for Content based Image Authentication

Jayashree S Pillai and T. Padma

Abstract--- The application of a number theory based pseudorandom sequence called Partial Quotient (PQ) sequence generated from the continued fraction expansion of irrational numbers in a semi fragile watermarking scheme for content based image authentication is considered in this paper. The generated pseudorandom PQ sequence is used to create sub vectors to be used at various instances in the watermarking process. The watermark is derived from the image and is embedded in the higher textured blocks. The watermarked images demonstrate high imperceptibility and make it suitable for use in artistic, medical and military applications where high quality and minimal distortion of the watermarked images is required.

Keywords--- Authentication, Watermarking, Continued Fractions, Irrational Numbers, Pseudorandom Numbers, Partial Quotients, Feature Vector, Key Vector

I. INTRODUCTION

AUTHENTICATION of digital media is the verification of the integrity of the media or asserting its copyright. With increased requirement for storing and transmitting information and the availability of advanced image processing tools, techniques are essential to establish the copyright and/or integrity of the image. This can be achieved using signatures or by watermarking. In certain applications like healthcare, defence, evidence or artistry, it is important that the quality of the watermarked image is retained and at the same time it is robust to malicious manipulations.

Digital watermarking is a technique commonly used for authentication of media where the watermark is hidden in the media and later recovered to verify the identity of the owner or integrity of the media i.e., its authenticity. Digital watermarks can be an external image, logo or a content based watermark extracted from some salient features of the image. Watermarks may be classified as robust, fragile and semi-fragile based on the robustness of the watermark. Robust watermarks are used for copyright protection as they are highly tolerant to non-malicious image manipulations. Fragile watermarks are easily destroyed on the slightest manipulation and can be used in applications when strict integrity check is required.

Content authentication is the validation of content integrity and does not require exact verification. Semi-fragile watermarks are good for content authentication as they can differentiate between non-malicious manipulations like compression, variations in intensity and mild noise and malicious manipulations like cropping and cut and paste.

Any watermarking technique uses pseudorandom sequences to generate secret information or to scramble the watermark. This paper presents ParQuoSCI, a content based image authentication scheme in the DCT domain that uses pseudorandom sequences generated from continued fraction expansion of certain irrational numbers to scramble the watermark and watermarking locations. The sequences demonstrate random properties and can be used in cryptographic applications.

The scheme is robust to Jpeg compression up to a certain predefined level and some incidental operations like Gaussian and salt and pepper noise, histogram equalization, median filtering, low pass filtering and sharpening. The watermark is visually imperceptible and gives good quality watermarked images.

II. RELATED WORK

A. Continued Fractions

In mathematics, a continued fraction is defined in [27] as an expression obtained through the iterative process of representing a number as the sum of its integer part and the reciprocal of another number, then writing the other number as the sum of its integer part and another reciprocal, and so on. They offer a useful means expressing numbers and functions in mathematics and have also been used in computer algorithms for computing rational approximations to real numbers.

Author et al., [8] have used continued fractions to enhance the key space of a chaotic map to design secure cryptosystems. In [7] the same authors have used the random sequence generated to encrypt images. [9], [10] and [19] have used the properties of certain continued fraction expansions to design authentication protocols, stream ciphers and to generate e-
cash, but the process involves the use of very long keys, up to 5000 digits long, so that the required security is achieved. In [21], the authors have proposed the use of transcendental numbers as pseudo random generators in cryptography. That irrational numbers can be used in cryptography has been evidenced in patents [22] in this area.

B. Image Authentication

Author et al., [11] generated the watermark derived using mathematical invariant relationship of corresponding DCT coefficients between a pair of blocks before and after JPEG compression and selected it as the image feature. They have mathematically shown that the same quantization matrix is applied to each of the 8 × 8 DCT block of the image at the time of compression and hence the relationship between the corresponding coefficients will not change after compression.

Author et al., [3] proposed a JPEG quantization property for all further smaller quantization tables to authenticate an image.

Author et al., [12] presented a scheme to verify the authenticity of JPEG images using secret keys and a mapping vector to embed the signature. An encrypted feature vector extracted from the DCT coefficients of the image is embedded invisibly into the selected coefficients in the same domain. The feature vector is then extracted at the receiver end and verified for authenticity at the receiver end. The scheme is robust up to 80% JPEG compression and is sensitive to malicious attacks.

Author et al., [19] have proposed improvement to [11] using two properties Quantization Sum Invariant Property (QSIP) and Further Quantization Property (FQP) that always exist under JPEG compression. QSIP is used to extract the content based feature and embedded in the DCT coefficients. The verification is done using FQP.

Most of the image authentication algorithms, in literature, use some source of randomness to scramble the watermark or the image or both in order to enhance the security of the system. System generated random numbers or popular generators like the Linear Congruential Generator (LCG), Blum Blum Shub (BBS) or symmetric key based techniques are commonly used to generate randomness. In this paper, a sequence generated from the continued fraction expansion of certain irrational numbers is used to scramble the watermark and identify watermarking locations. This sequence has been tested for randomness and certain cryptographic properties in [29].

III. THE PROPOSED SCHEME

This paper proposes the application of a pseudorandom sequence called PQ sequence to watermark images for secure authentication in the DCT domain. The algorithm is semi-fragile and is tolerant to mild image processing operations.

The PQ sequences generated from the partial quotients of the continued fraction expansions have previously been analyzed by the authors for pseudo randomness in [29] and are used in three instances in the watermarking algorithm:

a) to determine \( n \), the number of low frequency DCT coefficients to be considered for determining the feature index
b) to generate the Key Vector \( KV \) which is used to scramble the derived Feature Vector \( FV \)
c) as a Selection Index \( SI \) to determine the mid frequency locations where the watermark is to be inserted.

The authentication procedure has four stages - 1) Generation of the PQ sequence 2) Generation and scrambling of the watermark 3) Watermark insertion and 4) Watermark verification.

A. Watermark Generation and Scrambling

Feature Vector Extraction

Algorithm

Considering a pair of blocks \((P, Q)\), the relationship between two quantized DCT coefficients, \( \text{DCT}_p(v) \) of block \( P \) and \( \text{DCT}_q(v) \) at the same coordinate position \( v \) will remain the same before and after compression [11]. This property has been used to generate the watermark. The algorithm for watermark generation is:

a) Divide the image into non overlapping 8x8 blocks and compute the DCT for each block.
b) Place blocks in into two disjoint groups A and B based on a secret value and form pairs of blocks \((P, Q)\), based on random value, using one from group A and the other from group B
c) For each pair of blocks \((P, Q)\), \( n \) low frequency DCT coefficients from region \( \beta 1 \), including the DC coefficient and \( n – 1 \) low frequency AC coefficients are selected. The number of coefficients \( n \) is determined based on a string of bits extracted from secret location \( L1 \) of the PQ sequence. The feature vector \( FV_{pq} \) for a pair of blocks \((P, Q)\), is computed as:

\[
FV_{pq} = \begin{cases} 
1 & \text{if } \text{DCT}_p(v) \geq \text{DCT}_q(v) \\
0 & \text{if } \text{DCT}_p(v) < \text{DCT}_q(v) 
\end{cases} 
\]

for \( v = 1..n \)

\( FV_{pq} \) is scrambled by XORing with the corresponding Key Vector \( KV \) to get \( SFV_{pq} \). The Majority bit \( M_k \) for each block pair is extracted and the string of Majority bits is the content based watermark for the image.
B. Watermark Insertion

The embedding is done in the high mid frequency coefficients $\beta_2$ of the block pair. Region $\beta_2$ is selected to ensure robustness to lossy compression and at the same time exploit the Human Visual System (HVS) properties to minimize distortion.

Algorithm

For each pair of blocks $(P, Q)$, the bits in the PQ sequence from secret location $L3$ are used to select the coefficients from mid frequency region $\beta_2$ for embedding. If $C(a_1, a_{i+1}, ..., a_\text{m})$ are the mid frequency coefficients and PQV is the chosen string of bits from the PQ sequence from location L3, those coefficients from C are selected where $PQV = 1$.

a) For the corresponding positions $(i, j)$ of the selected pair of blocks, the ratio of the coefficients is determined:

$$R(i, j) = \frac{(\text{sgn})P(i, j)}{Q(i, j)}$$  \hspace{1cm} (2)

b) This vector will be the side information to be shared with the authenticator in a secure manner.

c) Modify the amplitude of the corresponding coefficients to embed the watermark:

If $M_b = 1$, \begin{align*}
P(i, j) &= P(i, j) \times \alpha \\
Q(i, j) &= Q(i, j) / \alpha
\end{align*} \hspace{1cm} (3)

If $M_b = 0$, \begin{align*}
P(i, j) &= P(i, j) / \alpha \\
Q(i, j) &= Q(i, j) \times \alpha
\end{align*} \hspace{1cm} (4)

where $\alpha$ is the watermark strength factor and can be experimentally determined. It has a value larger than one and $\alpha = 1.2$ gives good imperceptibility in the experiments conducted. The ratio $R'(i, j)$ after embedding the $M_b$ will increase if $M_b = 1$ and decrease if $M_b = 0$.

d) The inverse DCT transform is taken to get the watermarked image $I^*$.

C. Image Authentication

At the receiving end, the watermarked image is verified for authenticity by a procedure similar to the embedding process:

a) Compute the Majority bit $M^*$ from the DCT of the 8x8 block pairs as in the watermark generation process and shown in figure 3.

b) Extract the embedded Majority bit $M^*$ using the relationship:

$$M^* = \begin{cases} 
1 & \text{if } R^*/R > 0 \\
0 & \text{otherwise}
\end{cases}$$ \hspace{1cm} (5)

Figure 1: Scheme for Watermark Generation and Embedding

Figure 2: $\beta_1$ Represents the Significant Regions used to Generate the Feature Vector. $\beta_2$ represents the High Mid Frequency Region to Embed the Feature Vector
where
\[ R(i,j) = (\text{sgn})P^-(i,j)/Q^-(i,j) \]  
(6)

\( R^- \) is the extracted ratio of the corresponding selected coefficients of the watermarked block pair \((P^-, Q^-)\), \( R \) is the secret side information of the computed ratio before watermarking.

c) The extracted and evaluated Majority bits \( M^- \) and \( M^+ \) are compared to determine the authenticity of the watermarked image \( I^- \).

IV. EXPERIMENTAL RESULTS

The proposed scheme is implemented using Matlab and standard test images like Lena, Mandril, Cameraman and Drawing room, medical image like MrI and natural images like Patterns, Rice and Pentagon of varying dimensions and representation formats like tiff, png and bmp are watermarked and evaluated.

A. Imperceptibility Analysis

i. Quality of the Watermarked Images

The quality metrics used to measure the quality of the watermarked image is PSNR – Peak Signal to Noise Ratio, PCC – Pearson Correlation Coefficient, MSE – Mean Square Error and SSIM – Structural Similarity.

PSNR represent the measure of peak error and is given by the sequence

\[ \text{PSNR} = 10 \log_{10} \left( \frac{255 \times 255}{\sum_{i=1}^{k} \sum_{j=1}^{k} [I(i,j) - I'(i,j)]^2} \right) \]  
(7)

Where \( I(i,j) \) is the original watermark and \( I'(i,j) \) is the watermarked image and \( k \) is the size of the image. The unit of PSNR is dB (decibel) and can take valued from 0 to infinity. If the value is high, the image quality is high.

MSE is also used to measure the quality between the origin and watermarked image. The lower the value of MSE, lower will be the error and is given by equation 7.

\[ \text{MSE} = \frac{1}{k \times k} \sum_{i=1}^{k} \sum_{j=1}^{k} [I(i,j) - I'(i,j)]^2 \]  
(8)

SSIM is a measure of similarity as perceived by the human visual system (HVS).

\[ \text{SSIM} = \frac{(2\mu_x \mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \]  
(9)

The tests results as in Tables 1and 2 demonstrate a very high level of similarity between the original and watermarked image. In this algorithm, the average PSNR value is around 52 dB (decibels) which indicate high quality watermarked image. The average value of SSIM is very close to 1 and the Correlation Coefficient is 1. All the parameters indicate good quality of the images after watermarking.

Table 1: Measures of Imperceptibility of Watermarked Images of Proposed Technique

<table>
<thead>
<tr>
<th>Watermarked Image</th>
<th>MSE</th>
<th>SSIM</th>
<th>PCC</th>
<th>Time to embed (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>0.015</td>
<td>0.99</td>
<td>1</td>
<td>0.01</td>
</tr>
<tr>
<td>Rice</td>
<td>0.016</td>
<td>0.99</td>
<td>1</td>
<td>0.009</td>
</tr>
<tr>
<td>Pattern</td>
<td>0.018</td>
<td>0.99</td>
<td>1</td>
<td>0.23</td>
</tr>
<tr>
<td>Pentagon</td>
<td>0.018</td>
<td>0.99</td>
<td>1</td>
<td>0.14</td>
</tr>
<tr>
<td>Pirate_512</td>
<td>0.018</td>
<td>0.99</td>
<td>1</td>
<td>0.03</td>
</tr>
<tr>
<td>Cameraman_512</td>
<td>0.017</td>
<td>0.99</td>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>Drawing Room_512</td>
<td>0.017</td>
<td>0.99</td>
<td>1</td>
<td>0.03</td>
</tr>
<tr>
<td>Average</td>
<td>0.017</td>
<td>0.99</td>
<td>1</td>
<td>0.07</td>
</tr>
</tbody>
</table>

Table 2: Comparison of PSNR (in dB) of Watermarked Images of Proposed Technique with other Techniques and its Measure after Extraction
B. Tolerance to JPEG Compression

The results of applying varying levels of JPEG compression for the watermarked images and then authenticating the compressed image is depicted in Figure 4. It can be observed that JPEG compression up to 60% quality can be considered acceptable where as compression above that will cause the image to be distorted and can be deemed as not authentic.

The efficiency of the algorithm in extraction of the watermark can be given by the percentage difference computed between the original and extracted watermark.

Table 3: Percentage of Blocks determined as Tampered for Various Levels of JPEG compression of Watermarked Images

<table>
<thead>
<tr>
<th>Watermarked images</th>
<th>Compression level of images</th>
<th>Tampered Blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>90% 80% 75% 60%</td>
<td>4.39% 7% 8% 13%</td>
</tr>
<tr>
<td>Rice</td>
<td></td>
<td>2.63% 3.9% 6.4% 8%</td>
</tr>
<tr>
<td>Living Room_512</td>
<td></td>
<td>4.2% 7.2% 9.9% 13.0%</td>
</tr>
<tr>
<td>Pattern</td>
<td></td>
<td>5% 10% 12.6% 18%</td>
</tr>
<tr>
<td>Pentagon</td>
<td></td>
<td>3% 6% 7.2% 10%</td>
</tr>
<tr>
<td>Einstein</td>
<td></td>
<td>4% 7% 9% 14%</td>
</tr>
<tr>
<td>Mri</td>
<td></td>
<td>6% 11% 13% 16%</td>
</tr>
<tr>
<td>Mandril</td>
<td></td>
<td>1% 3% 4% 6%</td>
</tr>
<tr>
<td>Pirate</td>
<td></td>
<td>3.2% 7.2% 8.4% 11%</td>
</tr>
<tr>
<td>Cameraman</td>
<td></td>
<td>4.2% 7% 9.7% 17%</td>
</tr>
</tbody>
</table>

C. Tolerance to Incidental Distortions

The watermarked image is subject to incidental noises as mentioned in Table 4. The results demonstrate that the watermark is tolerant to mild image processing operations.

Table 4: Results after Extraction of Watermark from Images subject to Incidental Image Processing

<table>
<thead>
<tr>
<th>Attack</th>
<th>Lena – Grey Scale</th>
<th>Quality Parameter</th>
<th>Highest % Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaussian Noise</td>
<td></td>
<td>M=0 V=0.01</td>
<td>0%</td>
</tr>
<tr>
<td>Salt &amp; Pepper Noise</td>
<td></td>
<td>0.01</td>
<td>0.19%</td>
</tr>
<tr>
<td>Histogram equalization</td>
<td></td>
<td>0 - 200</td>
<td>0%</td>
</tr>
<tr>
<td>Median Filter</td>
<td></td>
<td>3x3</td>
<td>0%</td>
</tr>
<tr>
<td>Low Pass Filter</td>
<td></td>
<td></td>
<td>2%</td>
</tr>
<tr>
<td>Sharpening</td>
<td></td>
<td></td>
<td>1.2%</td>
</tr>
</tbody>
</table>

D. Efficiency Analysis

The major contribution towards the cost of the watermarking algorithm is the generation of the partial quotient sequences. The time taken to generate approximately 2,70,000 PQ sequences, which is the binary equivalent of 70,000 partial coefficient coefficients is given in Table 5.

Table 5: Measures of Time taken to Generate the PQ Sequences

<table>
<thead>
<tr>
<th>Irrational number</th>
<th>Extract 2,70,000 bits (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>√2</td>
<td>0.94</td>
</tr>
<tr>
<td>π</td>
<td>3.1422857</td>
</tr>
<tr>
<td></td>
<td>0.91</td>
</tr>
</tbody>
</table>

The cost of generating the partial coefficients can be evaluated to be \( O(\bar{d}^{1+\epsilon}) \), where \( \bar{d} = \max(\log_2(t_1), \log_2(h)) \) and \( \epsilon \) is a very small number. If \( r \) the number of partial coefficients to be computed is and if \( t_1 \) is the number composed by the first \( k \) digits of the irrational number \( \alpha \), then the cost of generation of the PQ sequence is \( O(r.\bar{d}^{1+\epsilon}) \).

2,70,000 is the maximum number of random bits that could be generated on a P4 system with 1GB RAM.

E. Security Analysis

i. Prediction of the Key Vector KV or Irrational Number \( \alpha \)

An attack will attempt to determine the secret irrational number used as the seed. It is not possible to predict irrational number \( \alpha \) even with the knowledge of a part of the partial coefficients produced due to the property of the continued fraction expansion.

As far as the Key Vector is considered, the probability of finding an equivalent key stream is very small as more than 2 lakh partial quotients were considered in the algorithm and a subset of the same, based on a secret value, was used to determine the Key Vector (KV). The results are discussed in [29].

ii. Collision Attack

The feature vector FV is extracted from more than one pair of coefficients. This makes it very difficult for an attacker to determine an equivalent image block to replace the watermarked one as FV is extracted based on the relationship between two blocks.

iii. Weak Key

Irrationals numbers generating periodic or predictable continued fraction expansion with predictable expansions can be avoided as they can create an inherent weakness in the pseudorandom sequence. But this can still be circumvented as in the proposed algorithm, more than 2,70,000 random bits are generated and the selection of the bits for the Key Vector KV is done from a secret position from amongst the bits, making it still secure [29].

iv. Precision of Irrational Number

The number of digits of the irrational decimal used must follow the same precision by both the sender and the receiver [29]. A single digit change or altering the precision by a digit can alter the partial coefficients generated. This requires exact precision of the software and architecture at the embedding and verification ends. But this can also be considered an advantage against the attackers, because even with the exact knowledge of the software and architecture of the system used to generate the continued fractions, inaccurate precision in the choice of the seed will make difficult to predict the PQ sequence.

V. CONCLUSION AND FUTURE ENHANCEMENT

Continued fraction expansion of some irrational numbers demonstrates random properties and can be used as pseudo random sequences. This proposed research work exploits the property of an irrational number to generate unique and infinite PQ sequences and is applied to a semi fragile watermarking algorithm to authenticate images that may be JPEG compressed up to a certain quality factor. The feature vector is derived from the relationship between the corresponding DC and selected AC coefficients of each pair of
blocks of the image and are used to embed the difference of selected DCT coefficients in the mid frequency domain so as to not cause visible distortions. The coefficients to be embedded are also selected from the PQ sequence. The quality of the watermarked images is quite good compared to [11]. The algorithm can be used in artistic, military and medical applications where it is necessary to ensure the originality and quality of the image after watermarking. As a further extension of the work, the scheme is to be tested for robustness to malicious attacks.

REFERENCES


