REGULAR PAPER

Random number generation using magnetic domain images of magneto-optical materials

To cite this article: Takuya Kawashima and Shinichiro Mito 2020 Jpn. J. Appl. Phys. 59 SEEA07

View the article online for updates and enhancements.
Random number generation using magnetic domain images of magneto-optical materials

Takuya Kawashima* and Shinichiro Mito

National Institute of Technology, Tokyo College, Hachioji, Tokyo 193-0997, Japan

*E-mail: mito@tokyo-ct.ac.jp

Received August 10, 2019; revised October 31, 2019; accepted January 16, 2020; published online February 4, 2020

Random numbers were generated from magnetic domain patterns of a magneto-optical (MO) material. A hundred thousand chaotic magnetic domain images were photographed by a transparent polarization microscope. Post data processing (binarization, frequency adjustment, exclusive-OR, and offset data reduction) was used to obtain a random number from the images. The generated random numbers passed the statistical test (NIST SP-800-22). This result could contribute to realizing a relatively simple and fast random number generator using MO materials.

© 2020 The Japan Society of Applied Physics

1. Introduction

High quality and fast random number generation is important for cryptography, scientific simulations, computational finance and fundamental physics tests and so on.1–4 In computer science, pseudorandom number generators (PRNGs) are widely used because they are easy to implement at low cost.5–10 However, output of PRNGs have strong long-range correlations because it is generated from a finite seed (prerecorded random number) by deterministic algorithm. Such correlations may cause unexpected errors in applications of random number. Therefore, physical (true) random number generators (RNGs) are needed.

RNGs have noise sources based on nondeterministic physical phenomena such as single photon transmission through half mirrors, breakdown current of metal oxide semiconductor structures, chaotic laser oscillation and so on.11–14 In principle, random numbers are generated from such unpredictable noise sources that have no periodicity. High-performance RNGs need good noise sources which is random and can be generated at high speed.

A magnetic domain pattern of the magneto-optical (MO) materials is promising phenomena for the noise source of RNG. It is chaotically formed by a result of interaction between thermally disturbed magnetic moments, and changes rapidly (∼GHz) by the application of a magnetic field.15–20 Furthermore, it is easily observed as a monochrome image with high contrast, which allows for a variety of post data processing by image processing.21–23 A fast and small RNG could be realized by using such characteristics.

The goal of this research is to realize a high-performance RNG using MO materials. In this paper, we report that the random number generation from the magnetic domain pattern images of single crystalline yttrium iron garnets (YIG).

2. Experimental methods

The experiment has three steps. The first step is capturing the magnetic domain image of the YIG. The next step is post data processing and binary sequence generation by image processing. The last step is statistical evaluation of the randomness of the sequences.

Figure 1 shows the schematic diagram of the experimental setup to obtain the domain images. It consists of a sample (single crystalline YIG films), a solenoid coil and a polarizing microscope. A magnetic domain pattern of the sample is photographed in the following procedure. It is performed continuously in 0.3 s per cycle.

1. A magnetization of the sample is saturated by applying a magnetic field from the coil. The magnetic domain pattern is erased.
2. Turn off the coil to weaken the magnetic field. The magnetic domain pattern is generated again.
3. The magnetic domain pattern is photographed by the polarizing microscope.

Figure 2 shows the block diagram of image processing flow for generating binary number sequences from photographed magnetic domain images.

In Fig. 2, the binarization unit is a simple thresholding defined by Eq. (1), where $I_{in}(x, y)$ and $I_{bin}(x, y)$ are the input and output pixels of the unit, and $t$ is a constant threshold.25,26 The purpose of this process is to remove signals (e.g. quantization noise etc.) other than the magnetic domain pattern contained in the input image.

$$I_{bin}(x, y) = \begin{cases} 0, & I_{in}(x, y) < t \\ 1, & I_{in}(x, y) \geq t \end{cases}$$

(1)

The frequency adjustment unit is implemented by the morphological transformation defined in Eqs. (2) and (3), where $I$ is the input image, $K$ is the kernel of 4-neighbor, and $k$ is the element of $K$.27–28 If there are more 0 pixels than 1 pixels of the input image “dilation” is applied, otherwise “erosion” is applied. The purpose of this process is to equalize the number of 0 and 1 pixels while maintaining the tendency of the domain pattern.

$$dilation: I \ast K = \bigcup_{k \in K} (I)_{-k},$$

(2)

$$erosion: I \ast K = \bigcap_{k \in K} (I)_{-k}.$$  

(3)

XOR processing is often used to increase the randomness of the noise in random number generation. In Fig. 2, this process is defined by Eq. (4), where $I_{ad}(x, y)$ and $I_{cor}(x, y)$ are the input and output pixels of the unit, and $n$ refers to the current process and $n - 1$ refers to the previous process.29

$$I_{cor}(x, y)_n = I_{ad}(x, y)_n \oplus I_{cor}(x, y)_{n-1}.$$  

(4)

The mask creation unit generates a mask that will be used later based on the conditions given by Eqs. (5) and (6), where
\[ I(x, y) \text{ and } I_{\text{mask}}(x, y) \text{ are the input and output pixels of the unit, } n \text{ refers to the current process, } -l \text{ refers to the process } l \text{ times before, and } A_n \text{ counts changes in pixel for the past } l \text{ inputs. } \]

\[ I_{\text{mask}}(x, y)_n = \begin{cases} 0, & A_n = 0 \\ 1, & A_n \neq 0' \end{cases} \quad (5) \]

\[ A_n = \sum_{m=n-l}^{n} \{I_{\text{ad}}(x, y)_m \oplus I_{\text{ad}}(x, y)_{m-1}\}. \quad (6) \]

The extraction unit generates a binary sequence by using the output of the previous unit. This process is described as Eq. (7), where \( I_{\text{ad}}(x, y) \) and \( I_{\text{mask}}(x, y) \) are the input pixels of the unit, and \( S \) is the output sequence

\[ S = \{I_{\text{ad}}(x, y) | I_{\text{mask}}(x, y) = 1\} \quad (7) \]

The generated sequences were evaluated by SP 800-22 which is a statistical test of random numbers provided by NIST (National Institute of Standards and Technology).30)

3. Results and discussion

Figure 3 shows some of the photographed magnetic domains. They are arranged from top left to bottom right in the order of photographed. Although there are stable patterns in the images because of the defects of the film, the all images were different and so they could be used as the noise source of RNG. The image size and the captured area on the sample surface is 640 × 480 pixels and \( 3 \times 2 \text{ mm}^2 \) respectively. the 100 000 images were taken for RNG. The black and white areas of the obtained images are not equal. Therefore, white area was widened to equalize the areas by a morphological operation. The equalized images were sequentially XORed with the last processed image. Then, stable patterns were removed by a mask process. These equalization and mask process are not necessary with a good-crystalline low-coercivity magnetic garnet. Their magnetic domains are naturally equalized for minimize the magnetostatic energy. In our case, the sample have defects and high coercive force. Therefore, we need the extra post processing. Nevertheless, obtained images were enough as a noise source of RNG.

Figure 4 shows an image of the generated sequence. The sequence size is about 1MB. Each pixel of the image corresponds to each byte of the sequence. That is, each pixel takes any value from 0 (Black) to 255 (White). And they are arranged from left to right and from top to bottom in the image. In the image, there is no clear pattern showing regularity in the sequence. Therefore, it is considered that the deviation of the magnetic domain pattern and the local periodicity have been removed by the post data processing. This process is not necessary if the YIG, which used as a noise source, does not have the ununiformity and stability on the domain pattern. It is considered that the post data processing will be further simplified by optimizing the YIG for the application for the RNG.

The results of the statistical randomness tests (NIST’s SP 800-22) of the sequence are shown in Table I. “Processed” is the result of the sequence generated by the proposed method. “Unprocessed” is the result of a sequence generated only by binarization of magnetic domain images (that is, the magnetic domain pattern itself). The sequence generated by the proposed method passed all 15 tests (all \( P \)-Values are bigger than the reference value of 0.01).
Hence, the processed sequence was statistically random. On the other hand, the sequence generated only by binarization failed in all tests. The $P$-Values were 0 that indicates that the unprocessed sequence is completely non-random. This result implies that the post-process is necessary for generating a random numbers. In this study, the images were simply XORed. The $P$-Value could be enlarged by a bit-shift or image rotation. According to these results, it is considered that a RNG using MO material as a noise source can be realized.

4. Conclusions

The random numbers can be generated from magnetic domain images of YIG films by post data processing. This

<table>
<thead>
<tr>
<th>Statistical test</th>
<th>Processed $P$-value</th>
<th>Result</th>
<th>Unprocessed $P$-value</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>0.71</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>Block frequency</td>
<td>0.04</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>Runs</td>
<td>0.55</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>Longest run</td>
<td>0.99</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>Rank</td>
<td>0.68</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>DFT</td>
<td>0.47</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>Nonoverlapping template</td>
<td>1.00</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>Overlapping template</td>
<td>0.84</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>Universal</td>
<td>1.00</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>Linear complexity</td>
<td>0.46</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>Serial</td>
<td>0.46</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>Approximate entropy</td>
<td>0.72</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>Cumulative sums</td>
<td>0.38</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>Random excursions</td>
<td>0.11</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>0.21</td>
<td>Pass</td>
<td>0.00</td>
<td>Fail</td>
</tr>
</tbody>
</table>

Fig. 3. Examples of the sequentially-obtained magnetic domain images of the single crystal YIG film. All images are different and so they could be used as the noise source of RNG.
technique could realize a fast and simple RNG because of its potentially fast random image generation.

Acknowledgments

This work was supported by JSPS KAKENHI Grant No. JP16K21569.

9) N. Ferguson and B. Schneier, Practical Cryptography (Wiley, New York, 2003), Chap.10.

Fig. 4. Grayscale image of the generated 1MB sequence.