Generation of frequency dependent digital chaos using FPGA

Sai Venkatesh Balasubramanian

Sree Sai Vidhya Mandhir, Mallasandra, Bengaluru-560109, Karnataka, India.
saivenkateshbalasubramanian@gmail.com

Abstract

Chaotic signals serve as ideal candidates as carriers in secure communication systems. The present work proposes the generation of a 'digital' chaotic signal using a frequency dependent iterative map. The proposed design is implemented using Field Programmable Gate Array and nonlinear characterization using Lyapunov exponent confirms the presence of chaos. A proof-of-concept communication system is then numerically designed and evaluated using the Mean Square Error, which reveals the sensitivity of the system to perfect decryption. The simplicity of the design, coupled with the high level of security obtained form the highlights of the present work.

Keywords: Frequency Dependent Chaos Generation, Digital Chaos, FPGA, Secure Communication

1. Introduction

In the current era of Big Data security forms key role and more over now a days , we mainly rely on secure communications [1]. With many communications taking place over long distance and mediated by technology, and increasing awareness of the importance of interception issues tells the importance of secure communication [2].Chaos is one of the best candidates yielding high security owing to its sensitive dependence on initial conditions [3].

The Present work purports to the generation of 'digital chaotic' signal using a frequency based iterative map. It is also demonstrated that, using the generated chaotic signal as a communications carrier increases the security.

Specifically, the present work implements the chaos generation using basic logical operations such as Exclusive OR (XOR) switching on four individual clocks with different amplitudes, frequencies and duty cycles. The above mentioned process is implemented using Very high speed integrated circuits Hardware Description Language (VHDL) in Field Programmable Gate Array (FPGA) where the system clock is used as the base clock and it is frequency divided with different ratios, to get different square waves with different frequencies and duty cycles. The generated chaotic signal is characterized using different parameters like Kolmogorov entropy (K2), Fractal Dimension (D2), Largest Lyapunov exponent (LLE) and Phase plane portrait. The main advantages of this work are

1. Simplicity - because of simple logical operations.
2. Security - due to high sensitivity of chaos to its initial conditions.

2. Theory

The definition of an iterative map is the primary step in chaos generation [4]. This map tells the behaviour of a system with respect to a control parameter 'R' [4]. The existence of Non-Linear region in an iterative map clearly indicates that for some values of control parameters, the system enters chaotic regions [5]. The iterative map function used in the present work is given by the equation:

$$f_o(i+1) = mod(f_o(i) + \frac{f_2}{f_1} - V(f_o(i)), \pi) \tag{1}$$

Here the f_o terms denote the output frequencies, whereas f_1 and f_2 denote the frequencies of the input signals. $V(f_o)$ denotes the input signal waveform employed in the chaotic system. The salient features of the above mentioned iterated function are as follows:

1. The frequency dependent components $f_o(i)$, $f_o(i+1)$ are present.
2. The control parameter is the input frequency ratio $R{=}f_2/f_1$.
3. The Signal dependent component $V(f_o)$ is present.

The bifurcation plot for a square input $V(f_o(i)){=}square(f_o(i))$ is given in Fig.(1).

From the diagram it is evident that control values close to non integral ratios such as 0.23, 0.31 and 0.42 give rise to chaos.

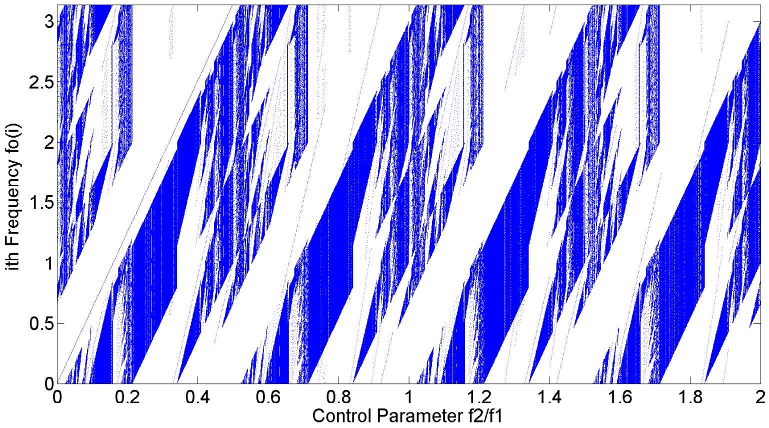


Figure 1: Bifurcation Diagram of the chaotic system with a square input

3. Hardware

The Basic design principles as obtained from the above equation are as follows:

1. Square wave input signals are given where, in addition to the amplitudes and frequencies, the duty cycles also have a significant effect on chaos.
2. The modulus function is implemented using basic logic operations such as XOR function (digital differential function) [6]. The schematic of this operation is illustrated in Fig.(2).

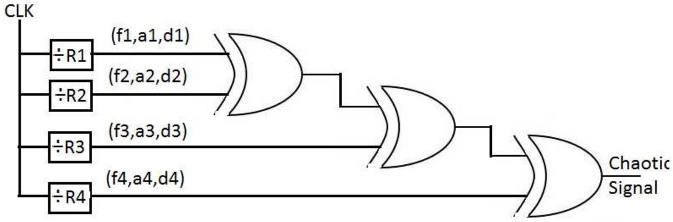


Figure 2: Block Diagram of the Chaos Generator

Out of the four signals $S1$, $S2$, $S3$, $S4$, one of the signals ($S1$) could be controlled by the user. This system is Implemented in Real time on an Altera Cyclone II-DE1 FPGA by implementing in VHDL as shown in Fig.(3). It is note worthy that the whole system is implemented using an extremely small number of logic elements 182, as shown in Fig.(4), which assertively establishes the simplicity of the system. The output format is represented in terms of 5 bits , the basic clock frequency used is 50 MHz and it is used as the sampling frequency. In accordance with Nyquist law, the highest among the four frequencies $f1$ is set to the half of the clock frequency [12].

4. Results

The four frequencies used are $f1$= 25 MHz, $f2$= 16.66 MHz, $f3$= 12.5 MHz, $f4$=10 MHz , amplitudes are $a1$= 15, $a2$= 11, $a3$= 15, $a4$= 11 and duty cycles in percentage are $d1$=66.66, $d2$= 50, $d3$= 40, $d4$= 33.33. The generated chaotic signal is shown in Fig.(5). The phase portrait gives information about chaotic dynamics and is shown in Fig.(6).

The chaos has been characterized using standard parameters given below:

1. Kolmogorov entropy represents the information content and is obtained as 7.839 bits/symbol [7].
2. Fractal dimension is a measure of self similarity and is computed using the Minkowski Bouligand Box Counting Method and is obtained as 0.852 [8].
3. Largest Lyapunov Exponent (LLE) is an assertive measure of these sensitive dependence on initial conditions and hence the security which forms the back bone of the present work [9]. It is computed using Rosenstein algorithm and is obtained as 30.3491 indicating high level of security [10].

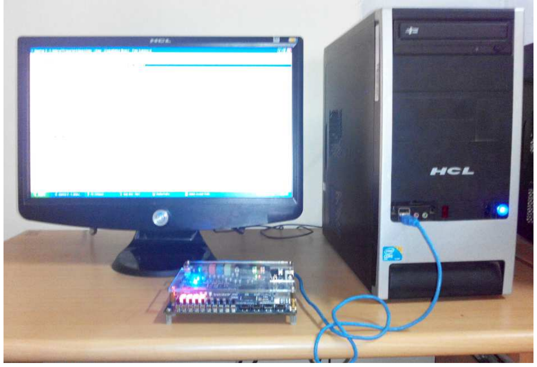
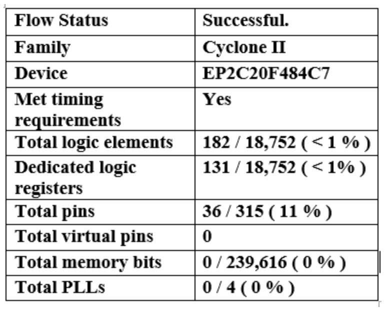


Figure 3: The Setup of Chaos Generation using FPGA



Flow Status	Successful.
Family	Cyclone II
Device	EP2C20F484C7
Met timing requirements	Yes
Total logic elements	182 / 18,752 (< 1 %)
Dedicated logic registers	131 / 18,752 (< 1%)
Total pins	36 / 315 (11 %)
Total virtual pins	0
Total memory bits	0 / 239,616 (0 %)
Total PLLs	0 / 4 (0 %)

Figure 4: FPGA Resource Utilization Details.

To characterize the security aspect of digital chaotic signal as a potential carrier, a random message bit stream is given in an additive embedding process with 18 dB Signal to Noise Ratio (SNR) calculated in MATLAB [11]. The MSE values at the de embedding side are compared for four cases, each corresponding to a mismatch in one of the properties of $S1$ as shown in Table 1 [11]. From the table it is evident that mismatches in the frequency, amplitude or duty cycle can increase the MSE by upto 63 Percent.

Table 1: Effect of Mismatch on Performance

Mismatched Parameter	Mismatch Percent	MSE Percent
Duty cycle	33.33	45.2455
Frequency	-33.28	29.7720
Amplitude	-10	62.1855
No Mismatch	-	0.0036

5. Conclusion

A frequency dependent iterative map is formulated for digital square wave inputs and the implementation of the map is done using XOR gates in an FPGA to generate digital chaos. The salient features of the implementation are as follows:

1. Four signals formed by dividing the FPGA clocks in different frequency ratios are used as the basis, and XOR based switching generates the required nonlinearity for chaos generation.
2. The FPGA implementation uses very less number of components, establishing the extreme simplicity of the proposed design.
3. Nonlinear characterization of the FPGA output using parameters such as Kolmogorov Entropy, Fractal Dimension and Lyapunov Exponent ascertains its chaotic nature.
4. The implementation of the digital chaos as a carrier in a prototype communication system yields extremely high values of security, with even slight mismatches in the amplitudes, duty cycles or frequencies at the receiver side causing MSE as high as 60 percent.

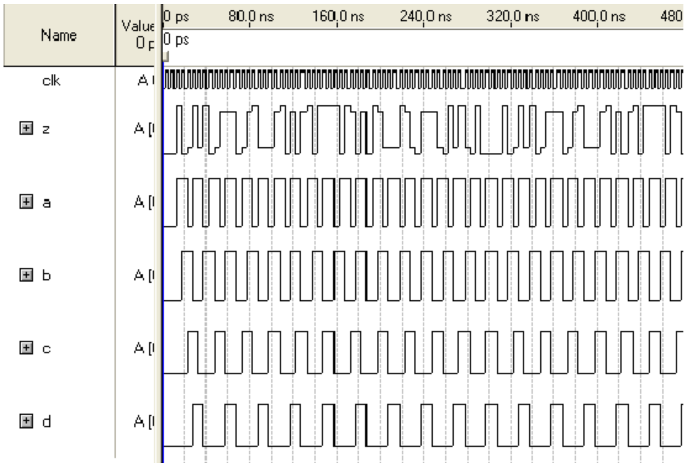


Figure 5: FPGA output waveforms. Top to Bottom: (System Clock (50MHz), Digital Chaos Generated, Clock $S1$, Clock $S2$, Clock $S3$, Clock $S4$))

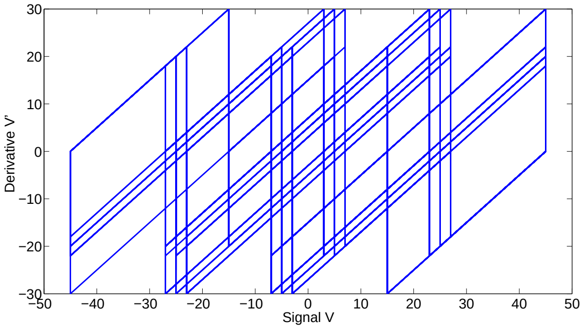


Figure 6: Phase Portrait of the Digital Chaotic Signal

The results established in the present work thus opens the doors for a radically new protocol: the protocol of Digital Chaotic Carrier - a protocol which can be implemented with extreme simplicity yet yields an enormous amount of security and fidelity, thus enhancing the quality of Big Data.

References

[1] Kocarev, L., Halle, K.S., Eckert, K., Chua, L.O., Parlitz, U.: 'Experimental Demonstration of Secure Communications via Chaotic Synchronization', *Int. J Bifurcation Chaos.*, 1992, **2**, p.709

[2] Young-Sik Kim., Jong-Hwan Kim., Sang-Hyo Kim.: 'A Secure Information Transmission Scheme With a Secret Key Based on Polar Coding', *IEEE Communications Letters.*, 2014, **18**, pp.937-940

[3] Lakshmanan, M., Murali, K.: 'Synchronized Chaotic Systems and Secure Communication', *Chaos in Nonlinear Oscillators: Controlling and Synchronization.*, 1996, **13**, pp.235-283

[4] Xiaowu Wang., Ronnie Mainieri., Lowenstein, J.H.: 'Circle-map scaling in a two-dimensional setting', *Phys. Rev. A.*, 1989, **40**, p.5382

[5] Bilotta, E., Pantano, P.: 'A gallery of Chua attractors', *World Scientific.*, Singapore, 2008

[6] Monica Borda.: 'Fundamentals in Information Theory and Coding', *Springer.*, US, 2011

[7] Latora, V., Balanger, M.: 'Kolmogorov-Sinai Entropy Rate versus Physical Entropy', *Phys. Rev. Lett.*, 1999, **82**, p.520

[8] Maragos, P., Maragos, F.K.Sun., Petros., Fang-Kuo Sun.: 'Measuring the fractal dimension of signals: morphological covers and iterative optimization', *IEEE Trans. Signal Processing.*, 1993, **41**, pp.108-121

[9] James, R.G., Burke, K., Crutchfield, J.P.: 'Chaos forgets and remembers: Measuring information creation, destruction, and storage', *Int. J Bifurcation Chaos.*, 2014, **378**, pp.2124-2127

[10] Rosenstein, M.T., Collins, J.J., De Luca, C.J.: 'A practical method for calculating largest Lyapunov exponents from small data sets', *Physica D.*, 1993, **65**, pp.117-134

[11] Jay Jacobs., Bob Rudis.: 'Data-Driven Security: Analysis, Visualization and Dashboards ', *Wiley.*, Indiana, 2014

[12] Walden, R.H.: 'Analog-to-digital converter survey and analysis', *IEEE Journal on Selected Areas in Communications.*, 1999, **17**, pp.539-550