IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 46-49
www.iosrjournals.org

Steganography Based on Low Power Linear Feedback Shift Register’s

Rehna Abdul Salam[1]&Elza Baby[2]
[1](Dept of E&TC Engineering, VESIT, Mumbai University,(MS),India)
[2](Dept of E&TC Engineering, KVNNIEER, SPPU,(MS),India)

Abstract-*The linear feedback shift register is a core component in many electronics applications. A design modeled around LFSR often has both speed and area advantages over a functionality equivalent design that does not use LFSR's. But it is having a drawback in the area of power consumption. This is overcame in this project by adding clock-gating and then the power efficient LFSR is applied in a steganographic circuit. Steganography is a very relevant field now as the need to protect information is very important. Steganography is the art and science of hiding information by embedding messages within a cover. It hides the presence of messages and creates a covert channel. The normal image steganography approach is modified and is made very secure by the addition of two new modules in this project. The newly introduced modules are the message bit randomizer and the pixel interleaver. The steganographic approach proposed here with low power LFSR's is a very power efficient and secure one.*

Keywords- *LSB steganograph, Built-in self-test (BIST), linear feedback shift register (LFSR)*

I. Introduction

In recent years, the design for low power has become one of the greatest challenges in high-performance very large scale integration (VLSI) design. As a consequence, many techniques have been introduced to minimize the power consumption of new VLSI systems. However, most of these methods focus on the power consumption during normal mode operation, while test mode operation has not normally been a predominant concern. However, it has been found that the power consumed during test mode operation is often much higher than during normal mode operation. Another category of techniques used to reduce the power consumption in scan-based built-in self-tests (BISTs) is by using scan chain-ordering techniques. These techniques aim to reduce the average-power consumption when scanning in test vectors and scanning out captured responses. Although these algorithms aim to reduce average-power consumption, they can reduce the peak power that may occur in the CUT during the scanning cycles, but not the capture power that may result during the test cycle (i.e., between launch and capture).

Mostly LFSR is used as random number generator to give random inputs for testing. So for any BIST application LFSR will be main design module.

1.1 Pseudo-Random Number Generator

Pseudo random number generator (PRNG) prevents invaders to find message bits easily. A secret key can be used as a seed for PRNGs. Using a seed causes PRNGs to generate the same random numbers on receiver side as on the sender side. In this paper, a linear feedback shift register (LFSR) is used as PRNG.

1.1.1 Implementation of LFSR

A LFSR is made of sequential shift-register with combinational feedback logic connected to it which can generate a sequence of binary values in a pseudo-random manner. A design modeled around LFSRs often has both speed and area advantages over a functionally equivalent design that does not use LFSRs.

Feedbacks around an LFSR’s shift register are connected to the certain points (taps) of LFSR construction and constitute either XORing or XNORing these taps to provide taps back into the register.

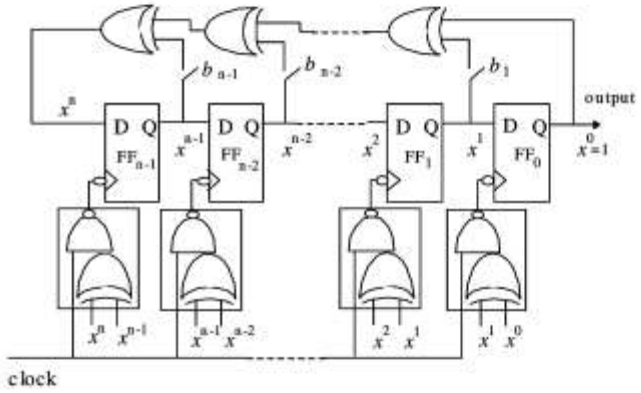
The selection of taps determines how many values can be generated in a given sequence before the sequence is repeated. Certain tap arrangement lead to maximal length sequences of (2n - 1).

1.2 Gated-clock Design of LFSRS

To reduce power consumption in a digital system a set of strategies termed dynamic power management (DPM) is often used. The DPMs strategy consists in disabling the logic circuits that are not performing functional operations during a particular time frame, thus reducing power consumption. [1]

At circuit level, this strategy is applied by the so-called “gated clock” approach which disables the clock of FFs More specifically, for FFswithout an enable signal,which is our case,we can adopt the strategy proposed in [5] and modified in [6], [7] as it is shown in Fig. 2. This is done by activating the FF only when the input signal is different from the actual output value. As itvcan be easily understood, this approach is perfectly compatible with a LFSR only adding some extra gates.[1] It is worth noting that the XOR and the NAND gates used to implement the gating can be implemented as a single gate (from hereinafter called XORNAND gate) as shown in Fig. 2. This is due to the complementary output always available in every FF.

To analytically evaluate the power consumption of the gated clock approach applied to a LFSR, we have to take into account also the dissipation introduced by the extra gates that are employed to implement the gated clock circuits, as well as the load effects introduced by these gates with respect to the traditional one.



.

Fig1. Gated-clock

In order to evaluate the power reduction obtained by applying the gated-clock approach to a LFSR, we have to analytically compare relationships (2) with (6). As a preliminary results, we obtained that..

$$C_{\mathrm{CK}} > \frac{\alpha}{1-\alpha}\Bigg(C_{\mathrm{inFF\_CK}} + C_{\mathrm{XORNAND}} + 4C_{\mathrm{inXORNAND}} + \frac{C_{\mathrm{INV}} + C_{\mathrm{inINV}}}{n}\Bigg)$$

which defines the technological condition (and the circuital so lutions for the gate’s implementation) so that the gate-clock approach leads to an improvement in terms of power reduction compared to the traditional LFSR implementation.

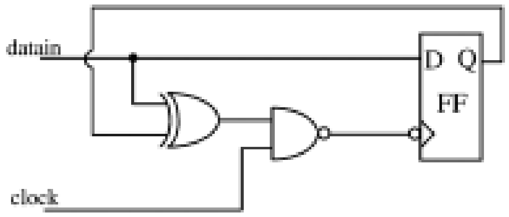


Fig 2. Block diagram of bit gated clock FF

II. Steganography

In the modern world, information is converted from paper type to digital information. Therefore, security improvement in data saving and exchanging is important. Different techniques of cryptography are used for data encryption but all of these methods can be recognized by invaders. If the information can be embedded in a medium in such a way that it cannot be observable easily, it will not raise the suspicion of invaders. This is the main idea of steganography.

The image formats used typically in such steganographical methods are lossless and the data can be directly manipulated and recovered. Since bmp images use lossless compression, one form of LSB attempts to use bmp images. However, other image formats are used as cover image as well.

2.1.1 Data hiding process:

Consider S = < x0, x1, … , xn > be the set of pixels of an image which is selected by a pseudo-random number generator. Pseudo random number generator produces random numbers according to the value of seed (stego-key). *x* is the gray value of each pixel. *n* is determined by the size of embedded message and the number of LSB bits in each pixel which can be used to embed messages. It can be calculated by:

$$n= k/m$$

Where *k* is the length of bit stream of embedded message, and *m* is the number of bits used to embed messages in each pixel.

2.1.2 Message Bit Randomizer Module

This part of design changes message bits so that if invaders find them, they cannot construct the message without access to secret key and the LFSR architecture. In each clock cycle, message bits must be XORed by a random number. The result of XOR operation will be embedded in pixels. At receiver side, extracted LSBs of each pixel must be XORed with the same random bits to construct the message bits.

A novel combinational randomizer is used for this reason. Figure 2 shows the architecture of this design. Message bits are embedded in least significant bits of a pixel[2]. A 16-bit LFSR with a seed (*seed2* input) generates random values. As shown in Figure 2, for one, two, three and four message bit insertion, four outputs (*y1, y2, y3, y4*) are considered. Input *m* value is changed from one to four by user selection and each value of *m* creates one of the outputs.

Module SHIFT16 contains a 16-bit LFSR that randomly generates sixteen bits in each clock cycle. However, these random values will not be XORed with message bits directly. Random bits from SHIFT16 module will be inserted in another module.

This module contains several multiplexers and LFSRs. In this module, if m=1, sixteen bits insert a 16 to 1 multiplexer. Selector of this multiplexer is connected to a 4-bit LFSR. Therefore, multiplexer selects one of these sixteen inputs as output, randomly. The output will be XORed by one message bit. This process is repeated for every bit insertion. Figure shows top level view of steg module which contains LFSR and multiplexer for one bit insertion.

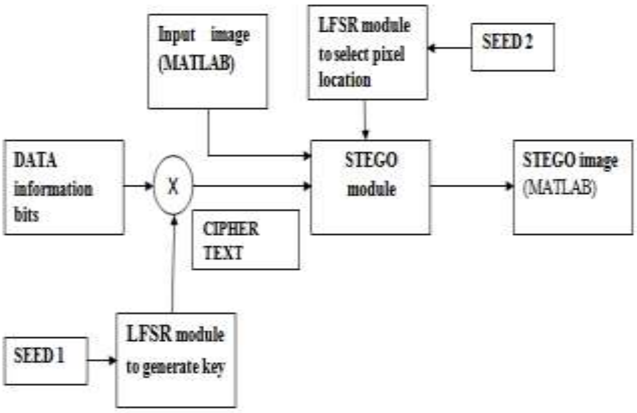


Fig 3. Block diagram of proposed stegnography method in functional mode.

III. Distortion Analysis

The images can be distorted in embedding process because of changing pixel bits.

Distortion is measured by means of two parameters namely, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

MSE can be calculated by

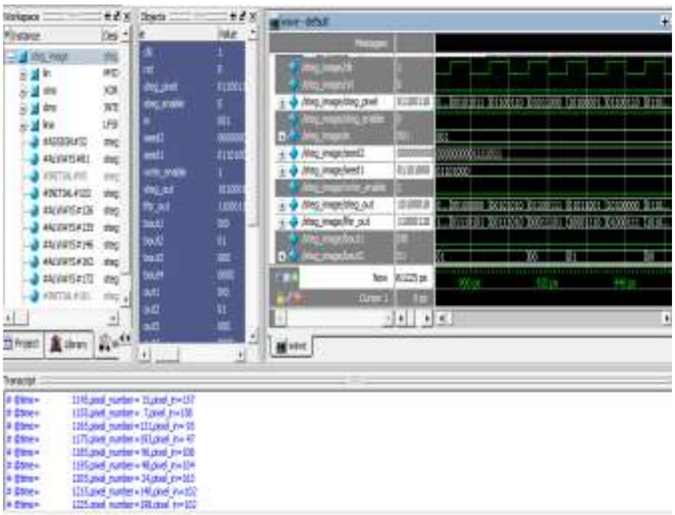
$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - Y_{ij})^2$$

The PSNR is calculated using

$$PSNR = 10\log_{10}\left\{\frac{I^2{}_{\max}}{MSE}\right\}dB$$

Imax is the maximum intensity value of each pixel which is equal to 255 for 8 bit gray scale images. Higher value of PSNR leads to better image quality. Results of steganography for Lena and Baboon digital images is represented in Figures 8 and 9 respectively and full embedding capacity is considered for m=1 to 4.

The size of these images is 256*256 pixels. As shown here, message embedding is done with no dramatic changes in image quality.



```
# @time=     1145,pixel_number= 15,pixel_in=137
# @time=     1155,pixel_number= 7,pixel_in=138
# @time=     1165,pixel_number=111,pixel_in= 95
# @time=     1175,pixel_number=163,pixel_in= 47
# @time=     1185,pixel_number= 98,pixel_in=108
# @time=     1195,pixel_number= 48,pixel_in=104
# @time=     1205,pixel_number= 24,pixel_in=163
# @time=     1215,pixel_number=140,pixel_in=102
# @time=     1225,pixel_number=198,pixel_in=102
```

Fig. 4. Simulated output

IV. Conclusion

A power efficient steganographic system with gated clock LFSR's is presented in this paper. Steganography techniques are more advantageous in terms of the security of the transmitted messages compared to any cryptographic methods. Furthermore, by using the pixel interleaver and message bit randomizer, protection against attacks is improved. User can select how many bits must be embedded in each pixel according to image quality and length of message. If the length of message is low, user can select one or two message bits to be embedded in each pixel. Otherwise, if the capacity is important and user needs to send more message bits, it can be satisfied by selection of more embedded bits in each pixel. This will allow the image quality and message capacity to be adjusted according to the user needs. In this design, two separate keys are used to improve security. This new approach can be considerd as a more improved one of steganography in terms of power and security.

References

[1] M Walter Aloisi and Rosario Mita "Gated Clock Design Of Linear Feedback Shift Registers*" IEE transactions on circuits and systems-II:Express briefs,vol.55,june 2008*

[2] Saeed Mahmoudpour and Sattar Mirzakuchakki "Hardware Architecture For A Message Hiding Algorithm With Novel Randomizers" *International journal of computer applications Vol.37, no.7,january 2012.*

[3] R. Jain, "The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation and Modeling:". *New York: Wiley, 1991.*

[4] R. David, "Random Testing of Digital Circuits. Theory and Application."*New York: Marcel Dekker, 1998[9]*

[5] S. Sannella ."Security Requirements for Cryptographic Modules" *U.S. Department of Commerce, National Institute of Standard and Technology, 2001, FIPS PUB 140-2.*

[6] L.Wang and E. J. McCluskey, "Circuits for pseudoexhaustive test patterngeneration," *IEEE Trans. Comput.-Aided Des., vol. 7, no. 10, pp.*