FPGA REALIZATION OF SPEECH SCRAMBLING USING SPARTAN-XL ELECTRONIC PLATFORMS

Dr. Mohammed N. Al-Turfi
Department of Computer and Software Engineering
University of Al-Mustansirya

Abstract: -

The Field Programmable Gate Array (FPGA) approach is one of the most recent category, which takes the place in the implementation of most Digital Signal Processing (DSP) applications. It had proved its capability to handle such problems and supports all the necessary needs like scalability, speed, size, cost, and efficiency.

In this paper a new circuit design is implemented for speech scrambling with an implemented example using FPGA is provided. In this implementation the speech coefficients are evaluated on both the scrambled and the De-scrambled sides.

This implementation was achieved using an FPGA Kit after building the logical circuits on the specified kit that uses the Spartan-XL electronic library type implemented using the ISE-4.1 software which is one of the latest versions of the Xilinx Foundation Series 2.1I software.

Key words: Security, Data hiding, Speech Scrambling, FPGA, Spartan XL.

استخدام تقنية (برمجة مصفوفات البوابات المنطقية) في تنفيذ الية اخفاء المعلومات الكلام بتطبيقها على رقاقات(SPARTAN-XL) الالكترونية

د. محمد ناصر الطرفي
قسم هندسة الحاسبات والبرمجيات
الجامعة المستنصرية – كلية الهندسة

الخلاصة: -

أن أتساع الحاجة الى الرقاقات الرقمية ذات السرع العالية و الحجم الصغير و التي تمتلك قابليات عالية في مجال معالجة المعلومات أصبح من المسائل الملحة التي تتسابق الشركات العالمية لأثبات قابلياتها في هذة المجالات و من هذة الشركات شركة زايلنكس و التي أثبتت حضور منقطع النظير خاصةة بعد تطويرها لرقاقة FPGA و التي أثبتت أنها الرائد في مجال معالجة الأشارة الرقمية بأعلى القابليات و أقل الكلف.

في هذا البحث تم تصميم دائرة بأستخدام هذة الرقاقة الغرض منها تغيير ماهية الكلام ليتسنى أخفاء المعلومات الحسية و لايمكن تحديدها ألا من خلال الدائرة الأخرى التي تقوم بعملية أعادة الكلام الى ما كان علية قبل أجراء عملية أخفاء المعلومات.

لقد تم تنفيذ التصميم باستخدام برنامج الـــ ISE4.1 و هو أحد النسخ المتطورة من برنامج Xilinx Foundation 2.1 المنتج من قبل شركة زايلنكس على الرقاقة الألكترونية نوع SPARTAN – XL

Introduction

Hiding, Scrambling, Encrypting, Coding…etc are the most important processes now a days since the type of wars is changed from the classical ones with bolts and guns to more effective and higher technology ones that uses information's and bits [Hussain,2000].

These great changes lead to change the type of data securing that fits these changes by using highly secured, complicated, large speed processing systems in order to be able to have the best response for such purposes [Hussain,2000].

The Field Programmable Gate Array (FPGA) technology was the remedy that takes the place in the fast electronic devices society and it had proved its fitness for handling tasks specialized with very fast, accurate, complicated processes. Where these tasks implemented with an exceptional efforts and costs. This lead to make these electronic kits are the new lead for a brand new branch in the designing of all digital systems specially the ones used for security purposes.

The last ten years, all the companies that deals with electronic device productions were in a race with each other's and time to be the initiative in the FPGA production field, because of the new word needs for this type of technology.

Recently, Field Programmable Gate Arrays have enjoyed widespread use due to several advantages related to relatively high gate density, short design cycle, and low cost. They can be used in all applications that currently use Small – Scale Integrated circuits (SSI), Medium– Scale Integrated circuits (MSI), Large Scale Integrated circuits (LSI), and Programmable Logic Devices (PLDs). They also replace Mask – Programmable Gate Array (MPGAs) in many applications that are limited to 10000 gates and they do not need a very high operational speed.[Hussain,2000]

Speech is the one of the most important type of data since nearly 90% of direct dealings and direct data exchange is represented by conversations and conferences which leads to secured them as possible specially secret and top– secret ones.

Since the amount of data in the speech specially for long periods of time is relatively large, then the circuit must have large capabilities and hence more complicated designs for transmitting and receiving the scrambled speech [1,2].

In this paper a new design for a circuit that can perform the speech scrambling on the transmitting and De-scrambling on the receiving sides are dedicated. The circuit operates in a high speed (Operating frequency is 1GHz). Short processing time and high accuracy (32 bit for the data 4 bytes at a time and five for control bit). Receiving data in many ways whether its serial or parallel and produce data in serial or parallel which made the circuit can be used for general purposes easily on both the transmitting and receiving sides.

An example and experimental results that has been obtained from the processor is given and shown in this paper with circuit block diagrams to show the data flow and results on the circuit.

FPGA Developed Environments

The reason beyond choosing the FPGA for the implementation of nearly all the modern digital systems is its fitness for handling the high computationally expensive problems and cover its intensive need for the parallel processing or pipelining [3,4].

Therefore among the advantages of FPGAs some are: -

1. The replacement of the small-scale integrated circuits (SSI) and medium-scale integrated circuits (MSI) chips.
2. The availability of parts of the shelf.
3. Rapid turn around.
4. Low risk.
5. Some FPGAs have the ability of reprogramming.
6. Relatively low cost and flexible design.

But its relative long design cycle is a disadvantage because its design process generally requires nine steps as follow : -

1. Entering the design in the form of schematic, net list, logic expressions, or HDL (Hardware Descriptive Language).
2. Simulate the design for functional verification.
3. Mapping the design into the FPGA architecture.
4. Placing and routing the FPGA design.
5. Extracting the delay parameters of the routed design.
6. Re-simulating for time verification.
7. Generating the FPGA device configuration format.
8. Configuring or programming the device.
9. Testing the product for undesired functional behavior.

This long design cycle force the production companies to face a challengeble problem and hence force them to find suitable solutions. [5, 6, 7]

Solutions are divided into four categories. The first one is consist of using the schematic approach for designing, which is used if the design elements and the circuit branches are well defined and their functions are specified.

The second one is consist of using the Very high-speed integrated circuits Hardware Descriptive Languages (VHDL), where this category is used with looping or iterative processes.

The third one uses the Finite State Machine (FSM) which uses with the control circuits, which have small numbers of inputs and outputs.

Any of the above categories can be merged together to form a new combination for handling new jobs. For example, we can implement a control circuit in an FSM part to control the process flow of a certain function implemented using the schematic approach.

The fourth category uses the high level language which is called the SYSTEM C4 or SYSTEM C5 [8].

This branch is a wild force PCI plug in board with 5-15 Processing Elements (PEs) with a 1MByte imbedded memory attached to each PE, and other inter connectors like FIFO, Crossbars, Single Inline Modules Data (SIMD).

This board is installed by its installation software after its placement in the motherboard of the personal computer, where this kind of kits operate on 1,3,5,10,20,33,66 MHz clock frequency with large number of inputs and outputs and wide range of function control and implementation [Chan,2000].

Speech Scrambling

One of the most important strategies for data hiding that is used in data security category is speech scrambling. Speech scrambling that will be discussed in this paper will consider that 95% of the phone lines uses the 56KBit/Sec Fax-Modem where the speech sample consist of 8 bits and the maximum bit rate of the phone line is 64 KBit/Sec. (Assuming the last intelligent frequency component in the speech is 4KHz. Using Nyquest rate so we will have 8KSample/Sec. With 8Bit/sample will lead to have a bit rate of 64KBit/Sec.) [Gilbert,2003 and Shafer,1982].

Speech scrambling depends upon the implemented scrambling functions inside the processing circuit because as much as the scrambling function is complex its difficult to be broken. But at the same time it will be time consuming and in need for more operations to handle the task which leads to make the circuit in need for more processing power (this means that the design is in need for more electric power and high-speed components with more complex circuit design)[Gilbert,2003 and Figueroa ,2003].

In this paper speech scrambling is first performed by reversing the order of the bits of each sample. Then the system proceeds to perform the scrambling process on the modified sample. At the end of the process, the data will be ready to be transmitted.

On the other side, the data must be Re-scrambled in order to reverse the order of the bits of each sample and then retrieve the original sample where the speech data now are the same as the ones at the start of the process.

FPGA Simulation of Speech Scrambling Systems

This paper shows a new method for designing an FPGA digital circuit for the evaluation of the coefficients of speech scrambling implemented using the ISE-4.1 software produced by Xilinx Company for FPGA electronic kit productions which represents one of the most recent updates for the Xilinx Foundation Series 2.1i. Therefore the simulation process should pass through four stages as follow.

The problem formulation and function establishment represents the first stage. In this stage the general features of the problem are identified in order to specify the needs for the problem solution. In the other hand; the function establishment is very important to specify the necessary equipments and devices for function implementation where the limitations and boundaries are defined.

The second stage is represented by over coming the limitations and difficulties in a reasonable way keeping an eye to the over all cost. While the implementation of the function must be optimized as much as possible in order to specify the type of the FPGA kit, size, capabilities, frequency ranges, number of inputs and outputs, power consumption, scalability, and compatibility.

Operating the optimized designed kit represents the third stage. Generally in this stage two important problems are appearing, the first one is represented by the timing problem, which is the

most important. The second one is represented by the production of the undesired results and values through the operating process and the way to get rid of them where most of these values are produced due to the timing problem.

The fourth stage is represented by connecting the designed kit to the operating environment and search for its compatibility and the best ways for operating in the presence of other system equipments. Therefore it's preferred to choose the kit type, as near as possible to the type of other system equipment's in order to reduce the compatibility problems. Or if it's possible and not costly to change the whole system since the FPGA kits are relatively of low cost.

For the first stage, specifying the scrambling function represents the problem formulation where this function specifies the type of speech processing and the way of dealing with each bit of the speech sample

For the second stage, the FPGA kit for the implemented design is SPARTAN-XL .The SPARTAN-XL 1.8V FPGA gives high performance, abundant logic resources, rich features set, all at exceptional low price. This family contains seven members offers density range from 50000 to 600000 system gates with wide operating frequency range (500KHz – 2.5GhHz)[8,9], delivering more I/Os and other features per dollar than other FPGAs by combining advanced process technology with a streamlined architecture based on the proven Vertex-E. Features include Block RAM (288 K bit), Distributed RAM (221K bit), 19 selectable I/O standard, 4 DLL (Delay Locked Loop), Fast Predictable Interconnection means that successive design iteration continue to meet timing requirements [Chan,2000 and Gilbert,2003].

The third stage depending upon the type of application, its operating frequency, its operating speed, and its response time. For example if the system is dealing with speech signal then the highest possible frequency component does not accede 6KHz in any way. While in target identification the image verification must be real time and very accurate with a very high response speed for direction changing. Or if systems are not in need for high speed and have symmetry in their circuits architecture then these symmetric circuits can be combined in few ones and the operations may be performed in sequence, or else redundant circuits will be built to perform parallel processing or pipe lining to achieve the necessary operating speed

The fourth stage is represented by implementing the whole system from its receiving point to its transmitting point since the used kit is more than enough to handle this task from size, speed, accuracy, cost. So; building the whole system on the same kit reduces the compatibility problems to the minimum.

Demonstrated Example

In this system we have 5 control bits control the flow of the process. These bits prepare each stage to receive the data from the stage before it whenever the data are ready and the stages are in the best situation to perform the data exchange.

When the receiving Serial – In – Parallel – Out Shift register finish the reception process, the control circuit signal to the reversal latch to receive the data from the shift register in a reversed mode. Now when the data settle in the reversal latch the control circuit resets the shift register and enable the scrambling latch to receive the reversed data and scramble it.

The data at the output may be received in a parallel form or in a serial manner according to te application it self. **Figure (1)** shows the circuit designs. **Figure (2)** shows the circuit-timing diagram and the system output for the input applied to the circuit. **Table (1**) shows the bit stream response of the system from the bit entrance to their outlet.

Figure (3) shows part of the report prepared by the software gives full details about the kit resources and the amount used by the circuit design. At the De-scrambling side the circuit will De-scramble the bits in a parallel manner in the De-scrambling latch and they will enter the reversing latch in order to obtain the original speech samples. **Figure (4)** shows the De-scrambling circuit designs. **Figure (5)** shows the circuit-timing diagram and the system output for the input applied to the circuit. **Table (2)** shows the bit stream response of the system from the bit entrance until the circuit obtains the original speech samples.

Therefore the forward and backward speech scrambling phases can be represented by the flow charts shown in **Figure (6) & (7)** respectively:-

Conclusions

This paper is to propose a new circuit design for the implementation and evaluation of speech scrambling systems using the FPGA platforms.

In this type of designs we are not in need for the wide range of circuit design in which we reduce the cost. And because of the kit wide capabilities high speed, high accuracy, low cost, low power consumption, so the transmitting and receiving circuits may be implemented on the same platform.

Other advantages is achieved by overcoming the disadvantage of the conventional speech scrambling systems that suffers from, where the data may appears byte by byte (serially) or they may appear in parallel form. This needs no large circuit to handle this task or it needs a global synchronization to keep system accuracy where any simple combinational circuit can handle the job properly.

With all what had mentioned above, the high speed circuit can handle several tasks at a time because in many applications the speech bit rate is not in need for very high speed circuits to be 1GHz operating frequency which leads to implement Several– In – One tasks. These will reduce the time, place, cost, power, and complexity where the same circuit may occupy many speech channels at a time.

References

[1] Mohammad N.Hussain, "Speaker Recognition Based Upon Phonemes Using Wavelet Packet Transform" Msc. Thesis, University of Baghdad, department of electrical engineering, October 2000,.

[2] N. Rex Dixon & Thomas B. Martin "Automatic speech and speaker recognition " 1989.A volume in the IEEE press selected reprint series.

[3] L.R.Rabiner & R.W. Shafer "Digital processing of speech signal" Book , 1982.

[4] Lawrence Rabiner & Biing– Hwang Juang "Fundamentals of speech signals" Book, 1993.

[5] Piyush Jamkhandi, Amar Mukherjee, Kunal Mukherjee, Robert Franceschini, school of electrical engineering and computer science," Parallel H/W- S/W architecture for computation of multi- wavelet transform using RMF algorithm". Report , July 2003,

[6] Sarin George Mathen, thesis, University of Kansas,"Wavelet Transform based adaptive image compression on FPGA". Book , June 2000

[7] www.Xilinix.com, "Spartan-XL 1.8 V FPGA family: introduction and ordering informations". July 2003, Company Production Catalog.

[8] Pak K. Chan, University of California,"Digital Design Using Field Programmable Gate Array". Book , October 2000.

[9] John E. Gilbert , "Coding: theory and applications on FPGA". Book , September 2003,

[10] Miguel Figueroa , Chris Diorio, University of Washington , "A 200 MHz , 3mW,16-Tap Mixed –signal FIR Filter". Company Production Catalog , September 2003

Table (1) The Scrambling system bit flow table

Data Input	**Circuit Reversing and Scrambling**				**Data Output**	
10011001	**Bit - Reversing**	10011001	99	**Bit - Scrambling**	01000000	4O
10011001		10011001	99		11111111	FF
10011001		10011001	99		10111111	BF
10011001		10011001	99		00000000	OO

Table (2):The De-Scrambling system bit flow table

Data input		**Circuit Reversing and Scrambling**			**Data Output**	
01000000	4O	**Bit –De- Scrambling**	10011001	**Bit –Reversing**	10011001	99
11111111	FF		10011001		10011001	99
10111111	BF		10011001		10011001	99
00000000	OO		10011001		10011001	99

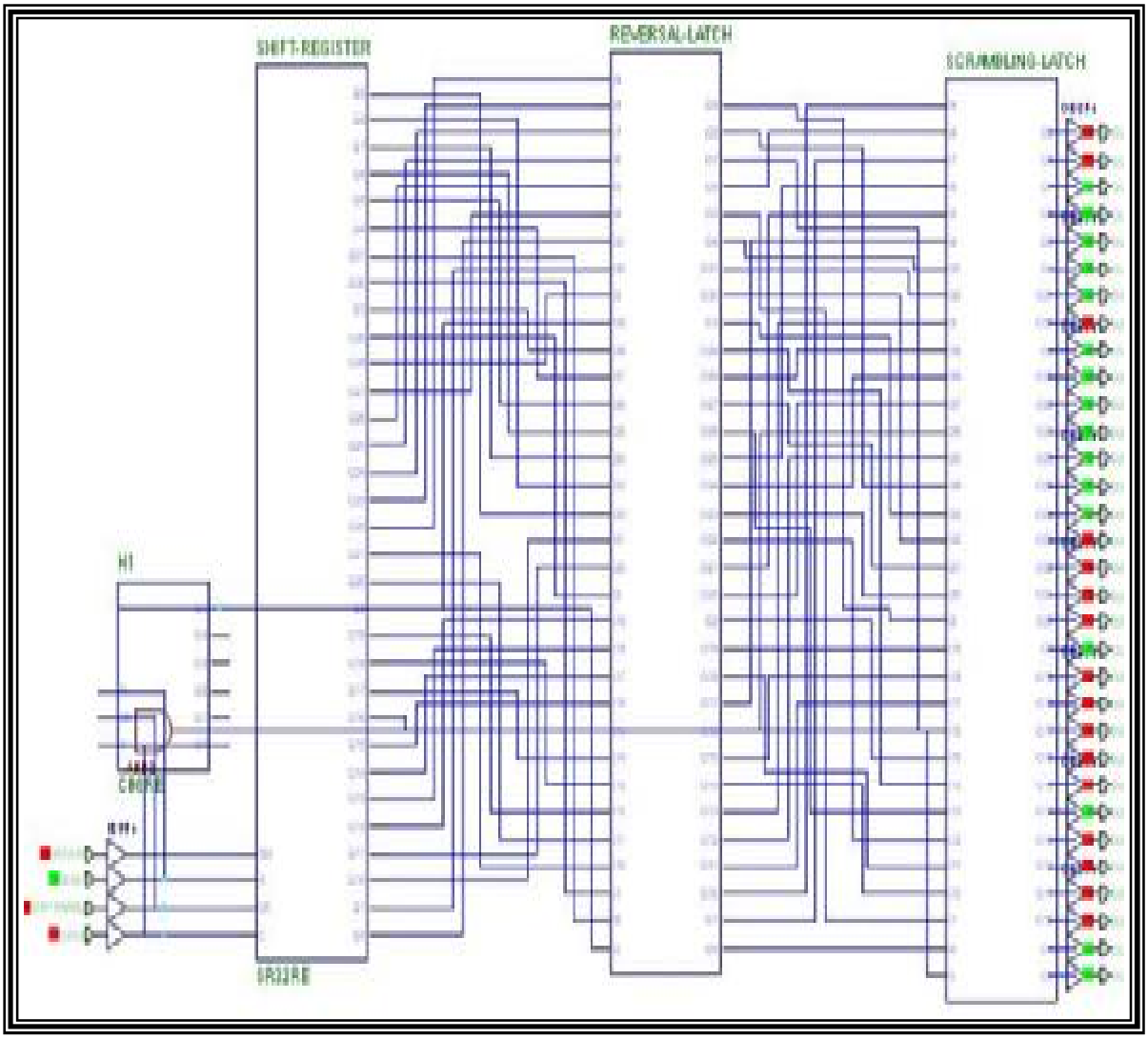

Figure (1) The circuit design for speech scrambling

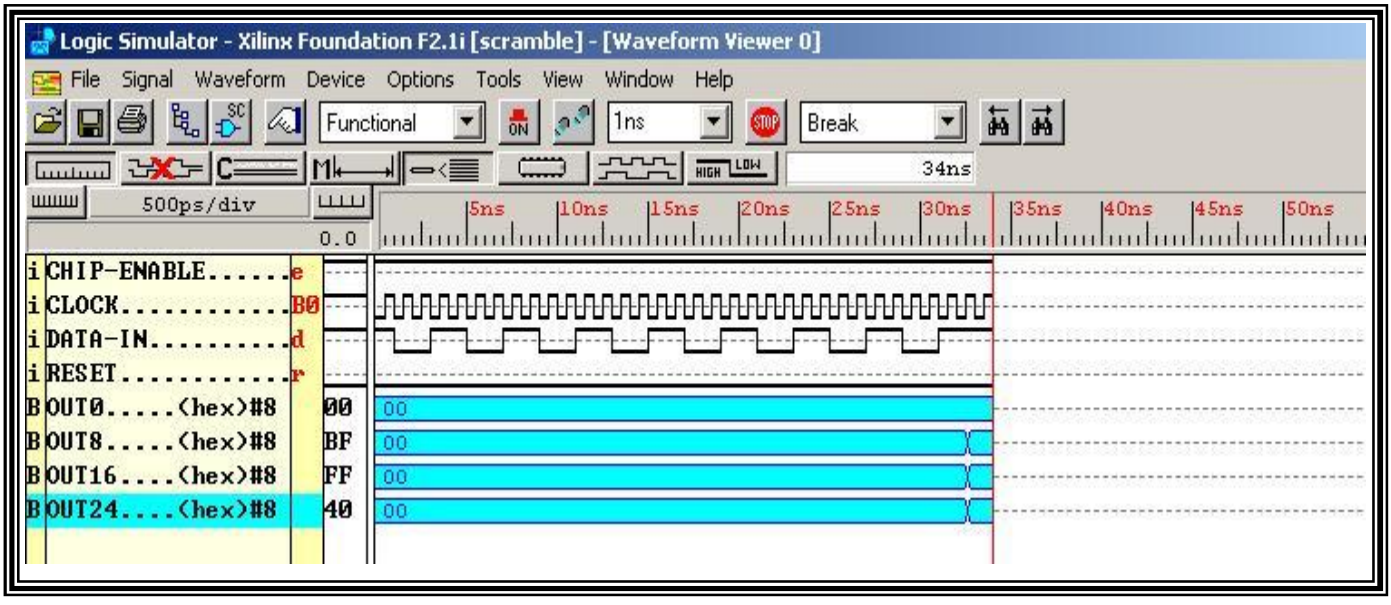

Figure (2):- Timing Diagram for the i/p & o/p data of the circuit

```
...
Reading component libraries for design expansion...

Annotating constraints to design from file "scramble.ucf" ...

Checking timing specifications ...

Checking expanded design ...
WARNING:NgdHelpers:359 -  The input pad net "CLOCK" driving one or more clock
   loads should only use a dedicated clock buffer (e.g., BUFG, BUFGP, BUFGS).
   This could result in large clock skews on this net.

NGDBUILD Design Results Summary:
  Number of errors:     0
  Number of warnings:   1
Removing unused logic...
Packing logic in CLBs...
   Running cover...
   Undirected packing...
Running physical design DRC...

Design Summary:
   Number of errors:          0
   Number of warnings:        2
   Number of CLBs:           86 out of    100    86%
      CLB Flip Flops:        38
      CLB Latches:           64
      4 input LUTs:          42
      3 input LUTs:           1
   Number of bonded IOBs:    36 out of     61    59%
      IOB Flops:              0
      IOB Latches:            0
Total equivalent gate count for design: 804
Additional JTAG gate count for IOBs:    1728
Writing design file "map.ncd"...

Removed Logic Summary:
 206 block(s) optimized away

Mapping completed.
See MAP report file "map.mrp" for details.

----------------------------------------------------
Resolving physical constraints.
Finished resolving physical constraints.

Device utilization summary:

   Number of External IOBs              36 out of 61      59%
      Flops:                             0
      Latches:                           0

   Number of CLBs                       86 out of 100     86%
Overall effort level (-ol):   2 (set by user)
Placer effort level (-pl):    2 (set by user)
Placer cost table entry (-t): 1
Router effort level (-rl):    2 (set by user)

Starting initial Placement phase.  REAL time: 0 secs
Finished initial Placement phase.  REAL time: 0 secs

Starting Constructive Placer.  REAL time: 0 secs
Placer score = 23820
Placer score = 15990
Placer score = 12120
Placer score = 10710
Placer score = 9090
Placer score = 6960
Placer score = 6570
Placer score = 6120
Placer score = 5670
Placer score = 5220
Placer score = 4920
Placer score = 4800
Placer score = 4140
Placer score = 3900
Finished Constructive Placer.  REAL time: 2 secs

Writing design to file "scramble.ncd".

Starting Optimizing Placer.  REAL time: 2 secs
Optimizing
Swapped  10 comps.
Xilinx Placer [1]   3630   REAL time: 2 secs

Finished Optimizing Placer.  REAL time: 2 secs

Writing design to file "scramble.ncd".

Total REAL time to Placer completion: 2 secs
Total CPU time to Placer completion: 1 secs

0 connection(s) routed; 343 unrouted.
Starting router resource preassignment
Completed router resource preassignment. REAL time: 2 secs
Starting iterative routing.
Routing active signals.
End of iteration 1
343 successful; 0 unrouted; (0) REAL time: 2 secs
Constraints are met.
Routing PWR/GND nets.
Power and ground nets completely routed.
Writing design to file "scramble.ncd".
Starting Cleanup
Improving routing.
End of cleanup iteration 1
343 successful; 0 unrouted; (0) REAL time: 4 secs
Writing design to file "scramble.ncd".
Total REAL time: 4 secs
Total CPU  time: 3 secs
End of route.  343 routed (100.00%); 0 unrouted.
No errors found.
Completely routed.
Total REAL time to Router completion: 4 secs
Total CPU time to Router completion: 3 secs

Generating PAR statistics.
Writing design to file "scramble.ncd".


All signals are completely routed.

Total REAL time to PAR completion: 4 secs
Total CPU time to PAR completion: 3 secs

PAR done.

================================================================
Timing summary:
---------------

Timing errors: 0  Score: 0

Constraints cover 391 paths, 111 nets, and 343 connections (100.0% coverage)

Design statistics:
   Minimum period:   8.243ns (Maximum frequency: 121.315MHz)
   Maximum combinational path delay:  12.061ns
   Maximum net delay:   9.088ns

WARNING:Timing - Clock nets using non-dedicated resources were found in this
   design. Clock skew on these resources will not be automatically addressed
   during path analysis. To create a timing report that analyzes clock skew for
Opened constraints file scramble.pcf.

Sat Mar 04 21:23:01 2006

Running DRC.
DRC detected 0 errors and 0 warnings.
Saving ll file in "scramble.ll".
Creating bit map...
Saving bit stream in "scramble.bit".

----------------------------------------------------

xcpy scramble.bit c:\fndtn\active\projects\scramble\scramble.bit

----------------------------------------------------
```

Figure (3) part of the report that prepared by the software about the circuit

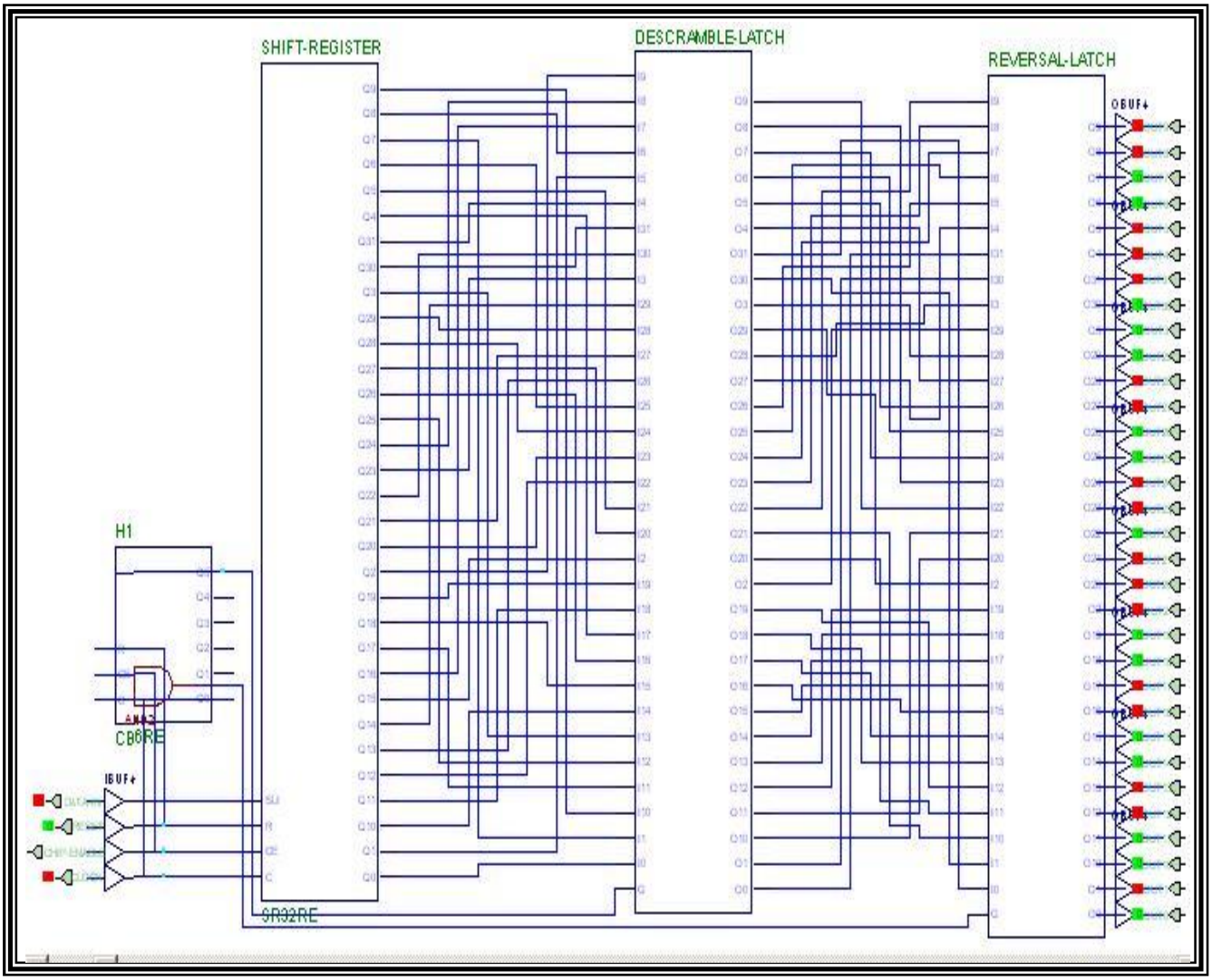

Figure (4) The circuit design for speech De-scrambling

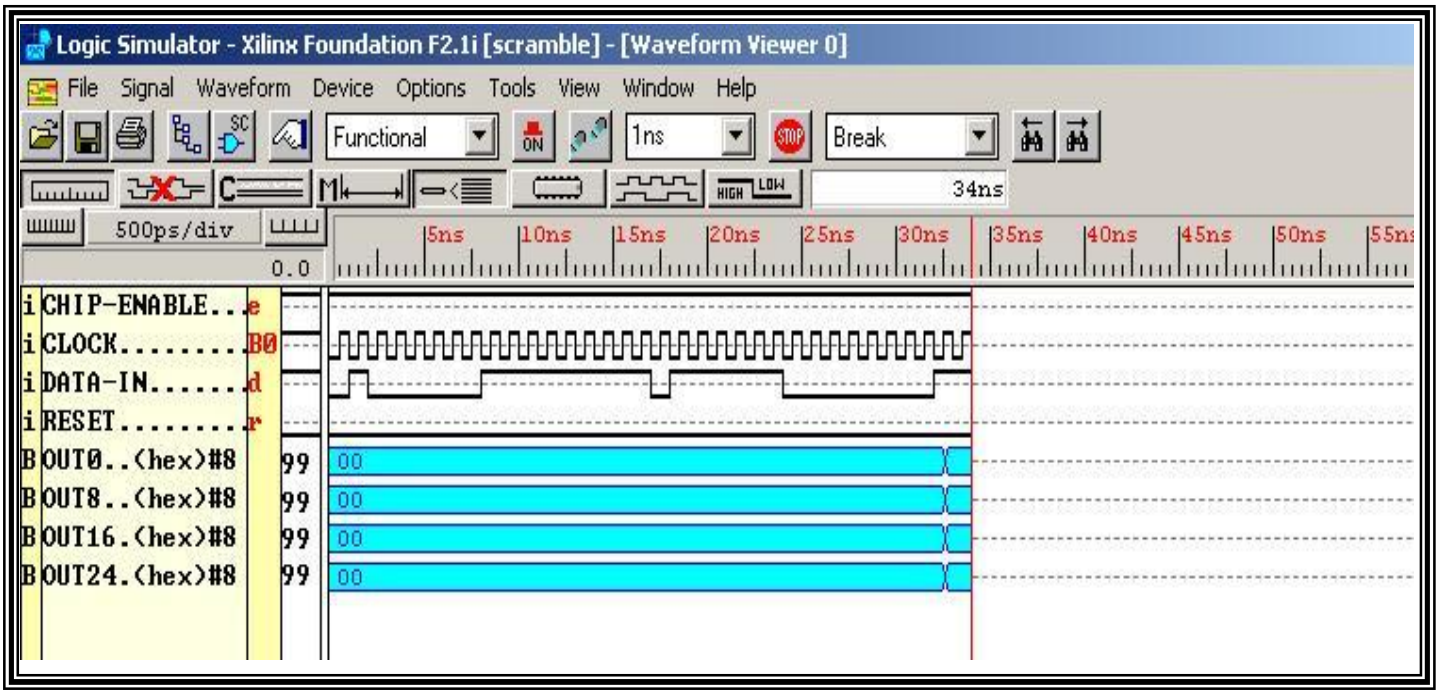

Figure (5) Timing Diagram for the i/p & o/p data of the circuit at the De-scrambling side

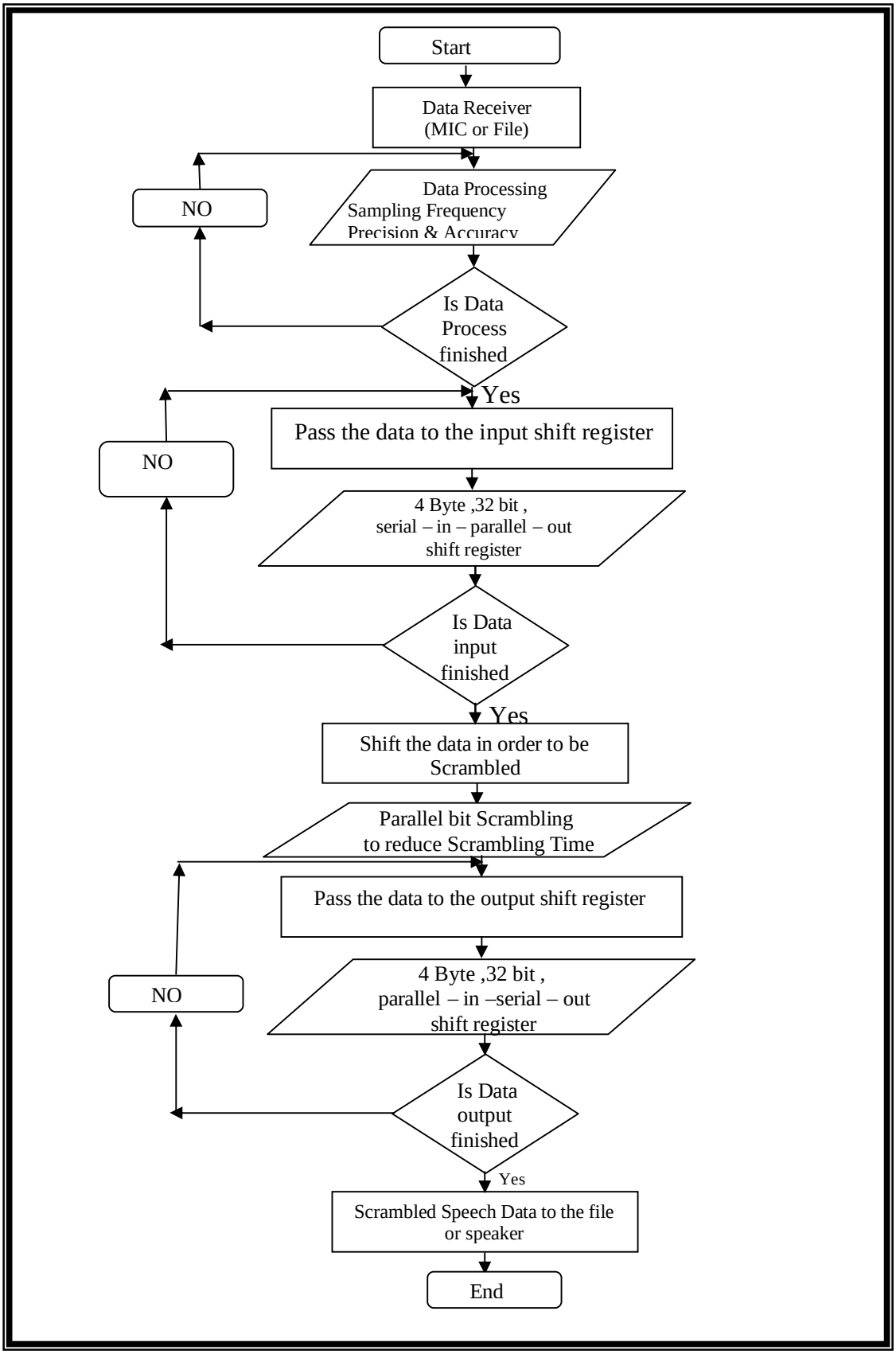

Figure (6) The forward phase of Speech scrambling process

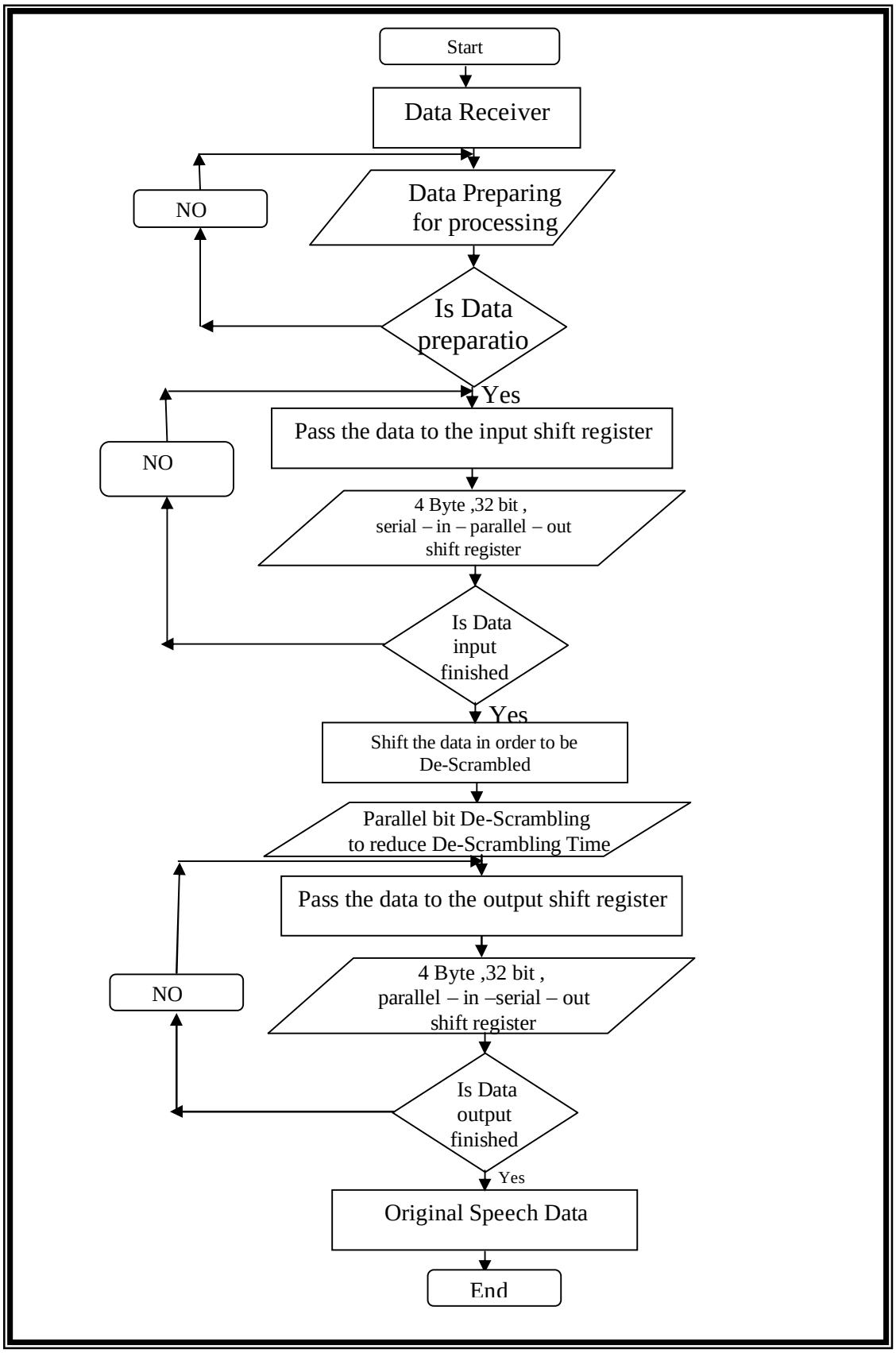

Figure (7) The backward phase of Speech scrambling process