High-speed Image Data Transmission And Comparison Based on ARM and FPGA

Sonawane Nilam R.¹, Prof. Galande S.G.²
¹M.E. student, ²Assistant Professor, P.R.E.C., Loni

Abstract— The high-speed image transmission and comparison based on ARM and FPGA is presented. The captured images store in software and hardware simultaneously. Transmission of these images to hardware through serial communication. And write this image data to FPGA. Then reconstructed this data for comparison of both the images which is store in software and hardware. FPGA is used to complete high-speed image data acquisition, through ARM to manage and control of FPGA.

Keywords— ARM, FPGA, LAN, Wireshark, serial communication.

I. INTRODUCTION

In the last 25 to 30 years, since the inception of personal computers, analysis of digital images has become a common place task in both the biological and industrial laboratory. As digital camera technology and microscopy have become more refined, the demands for more precise and accurate measurements from the resulting digital images have followed. These measurement demands include not only the physical image parameters, but also the color. This image either stored in hardware or software. But this project can store images in hardware or software simultaneously. We also added one thing that we can compare both this images. Here system does the pixel-by-pixel comparison. And also capture image when intrusion is detected. This image writes in FPGA through ARM. The comparison engine gets the color of pixels that have the same coordinates within the image and compares this color. There are some factors that affect image comparison and that may lead to unexpected comparison results. These are font smoothing, Image Size, Coordinates Offset, Screen Resolution, DPI Setting, Color Depth etc.

II. HARDWARE DESIGN

A. System Design

This design uses Phillips LPC2138 for the ARM chip and FPGA is SP601 evolution kit of Xilinx's Spartan series chips. Besides, System components include serial communication, memory and network driver, camera DLL. As shown in Figure.1.

We use internal or external camera to capture the image. This image can store in PC which is application software for camera, ARM, serial communication.

Here images store in software and hardware also. This system compares these images. Then it shows the result that images store in PC (Software) and hardware are same or not. When these images are store into hardware wireshark is used to check communication between PC and ARM. Then it writes in text format to SRAM of FPGA. Because image data consist of thousands of bytes. At the time of comparison image stored in SRAM will be read by software with the help of control signal generated by ARM. Here ARM uses serial communication. In this project user create code for capturing image and image comparison in VB.NET. VB.NET is a type safe language. There is no variant type in VB.NET and no type conversions happen automatically in VB.NET. In VB.NET you can create multithreaded applications. When user capture the image from internal web camera it simultaneously store in hardware and software. Then we call first image from software and second image from hardware and compare them.

B. Intrusion Detection System

In this system user add intrusion detection system (IDS), which capture image when any intrusion (paper, fingure) cut the infrared.
Fig.2 Intrusion Detection Application

Most of the system may stop an intrusion but not required or expected for real-time. Generally detection system (IDS) monitors system activities or policy violations and send reports to a management station. When any intrusion is detected in between these IRT and IRR (ex. we place the paper or figure in between two LEDs), then it captures the image. If IRT and IRR are not in front of each other then hyper terminal continuously transmits the ‘A’ character. Primarily focused to identifying some logging information, incidents to intrusion detection and prevention system. Also used for other purposes like security, documenting threats etc. There will be range limitation. If user extends the range this problem also reduces. Software bug, corrupt DNS data, local packets which create high false-alarm. It uses because if anybody pass from prohibited area, that will cut IR TxRx and capture the image. So in absence of monitor image store in hardware. It gives security application.

III. COMMUNICATION MODULE

A. Serial Communication

1. RS232

In 1962, RS232 was introducing. Generally electronic data communication between elements is divided into two categories: Single ended and differential ended. RS232 is single ended. This is renamed for use in industry. The RS232 interface common ground between DTE and DCE. Assume that when short cable connects the DTE to DCE, this may be different on buses with different ground or may not because of longer line and connection between devices. RS232 port supply limited power to another device. Important considerations are number of output lines, state of output line and type of interface driver IC. The type of driver ICs used in serial ports can be divided into following categories:

- Low power drivers which require +5V power supply. It has internal charge pump for voltage conversion such as many industrial microprocessor control
- Low voltage and low power drivers which meet EIA-562 standards such as notebooks and laptops.
- Drivers which require plus (+) and minus (-) voltage power supplies such as 1488 series of interface integrated circuits. (Most desktop and tower PCs use this type of driver)

RS232 data is bipolar. +3 to +12 volts indicate an “ON” or 0-state condition while -3 to -12 volts indicate “OFF” or 1-state condition. “ON” state may achieve with less positive potential. Modern computer equipment ignores the negative level and accepts “OFF” state or zero voltage level. So to drive the RS232 circuit’s 5 volts DC circuit is capable. The RS232 signals that transmitted/received reduce overall range. For dead area output level swings between +12V and -12V and +3 and -3 is designed to absorb line noise. Many receivers designed for Rs232 are sensitive to differentials of 1V or less.

2. MAX232

Output swing is guaranteed to meet the EIA/TIA232E and V.28 specification which calls for ± 5 v minimum driver output levels under worst case conditions. The typical driver output voltage swing is ±8 V when loaded with a nominal 5kΩ RS232 receiver and VCC=+5V. These include minimum 3KΩ load, maximum operating temperature and VCC=+4.5V. Input threshold are both CMOS and TTL compatible. Output voltage for unloaded driver ranging from (V+1.3V) to (V+0.5V). When 400KΩ input pull up register to VCC are built in then inputs unused driver can be unconnected.

Because of inverting drivers, the pull up register force output of unused drivers low. The internal input pull-up resistors to typical source 12μA, except in shutdown mode where the pull-ups are disabled. In shutdown mode, in three-state mode, or when power of device is removed, the drivers output turn off and enter a high impedance state where leakage current typically microamperes (25μA). Outputs can be driven ±15V. In shutdown mode power supply current drops up to 8μA. When in low-power shutdown mode, the driver outputs are turned off and there leakage current is less than 1μA with the driver output pulled to ground. The driver output leakage remains less than 1μA, even if the transmitter output is back driven between 0V and (VCC +6V).
Below -0.5V, the transmitter is diode clamped to ground with 1kΩ series impedance. The transmitter is also sneer clamped to approximately VCC+6V, with a series impedance of 1kΩ. Slew rate of driver output is limited which is less than 30V/µs as required by EIA/TIA-232E and V.28 specification. Typical slew rates are 10V/µs loaded and 24V/µs unloaded with 3Ω and 2500pF.

B. Wireshark

Wireshark initially developed by Gerald Combs. Wireshark used to check communication between PC and ARM. It is a network packet analyzer. It examines what’s going insides network cable. The network packet analyzer tries to capture network packets and try to display that packet data. In 2008, version 1.0 was arrived for wireshark. Its release coincides with first developer and user conference called sharkFest. Developer uses it to debug protocol implementation. Network security engineers use it to examine security problems. Also network protocol internals can learn. Available for UNIX and windows. Import and export packet data from and to lot of other capture programs. It search packet on many criteria. When data captured open and save packets. Also display packets with protocol information.

IV. CONCLUSION

This system gives more flexibility of ARM and the parallel of FPGA, that the design of high-speed data acquisition board. Also done the image comparison application. The board uses LPC2138 ARM chip. We capture the image from web camera and store it in software and hardware. At the same time write image to FPGA through ARM.ARM generated handshaking signal to write image data in FPGA in a text format. If user required image store in FPGA is read by software with the help of control signal generated by ARM. Again it reconstructed to compare with software image.

V. RESULT

If comport selection is proper, open the web camera. As acknowledgement receives from hardware or any intrusion is detected, it captures the image. Load first image from software and second image from hardware which is reconstructed. If all bits in data are same then system gives a result, “Images are same”. Otherwise any bit corrupted it gives a result, “Images are not same”.

REFERENCES