International Journal of VLSI System Design and Communication Systems

ISSN 2322-0929
Vol.02, Issue.07,
October-2014,
Pages:0524-0529

www.ijvdcs.org

FPGA Based Wireless Mobile Jammer

HAMEED MOHAMMED[1], V. PRATHYUSHA[2], K. ASHOKE BABU[3]

[1]PG Scholar, Dept of VLSI, Sri Indu College of Engineering & Technology, Ibrahimpatnam, Hyderabad, India.
[2]Assoc Prof, Dept of ECE, Sri Indu College of Engineering & Technology, Ibrahimpatnam, Hyderabad, India.
[3]Professor & HOD, Dept of ECE, Sri Indu College of Engineering & Technology, Ibrahimpatnam, Hyderabad, India.

Abstract: Mobile Jammer is one of the instruments used to prevent the cellular phones from receiving signals from Base Stations. Cell Phone Jammers are very useful to the society from the anti social elements by using the mobile jammers. So, in this paper we are designing a new Mobile Jammer unit which is capable of blocking the cell phone working not the signal receiving from Base Station, which make effective use of the situation where jammers actually used. By using the FPGA and RF technology to implement low cost jammers is implemented.

Keywords: Jammers, Mobile Jammer, FPGA, RF Transmitter, RF Receiver, LCD.

I. INTRODUCTION

Cell phones are everywhere these days. According to the Cellular Telecommunications and Internet Association, almost 195 million people in the United States had cell-phone service in October 2005. And cell phones are even more ubiquitous in Europe. A Mobile Phone Jammer is basically defined as a Device that stops any communication process within Phones. Due to the rising Number of Mobile Phone Subscribers, there are also rising concerns such as breach of privacy and cheating at exams in Schools/College/University. Mobile Phone Jammers are also use to disrupt communications by outlaws and rebels, which hampers their illegal and violent Operations. There are Mobile Phone Jammers that are designed to stop the Remote Capabilities of Mobile Phones from causing Improvised Explosive Device (IED) explosions by terrorists. As an Expert Mobile Phone Signal Jammer Supplier inside Integrated Marketing Services is providing Variety Mobile Phone Signal Jammers to Various.

Fig1. Mobile Phone

Normally Mobile Jammers are used in the Nursing Schools and Colleges to Maintain Discipline and Order within the Institution. Mobile Phones are wrongly utilized by Students in the Examination. Mobile Phone Jammers Mobile Phone Jammers Keep discipline in silent area like Class Rooms, Temples, masjid, gurudwaras and Meditation Center. In a Nursing College, Discipline and Duty with Silence is very necessary to Maintain Patient Security, Care and Hospital Management System. So all the Nursing Colleges has to train their Students with strict discipline of not using Mobile Phones inside the Nursing College Campus or inside the Class Rooms., We are providing Mobile Signal Jammers to prison, theater, conference center, library, church, gas station, school campus, Government Hospitals, and Military site etc.

II. INSIDE CELL PHONE JAMMERS

Electronically speaking, cell-phone jammers are very basic devices. The simplest just have an on/off switch and a light that indicates it's on. More complex devices have switches to activate jamming at different frequencies. Components of a jammer include:

A. Antenna

Every jamming device has an antenna to send the signal. Some are contained within an electrical cabinet. On stronger devices, antennas are external to provide longer range and may be tuned for individual frequencies.

1. Circuitry:

The main electronic components of a jammer are:

- **Voltage-controlled oscillator** - Generates the radio signal that will interfere with the cell phone signal.
- **Tuning circuit** - Controls the frequency at which the jammer broadcasts its signal by sending a particular voltage to the oscillator.

- **Noise generator** - Produces random electronic output in a specified frequency range to jam the cell-phone network signal (part of the tuning circuit).
- **RF amplification** (**gain stage**) - Boosts the power of the radio frequency output to high enough levels to jam a signal.

2. Power supply:

Smaller jamming devices are battery operated. Some look like cell phone and use cell-phone batteries. Stronger devices can be plugged into a standard outlet or wired into a vehicle's electrical system.

B. Jamming Basics

Disrupting a cell phone is the same as jamming any other type of radio communication. A cell phone works by communicating with its service network through a cell tower or base station. Cell towers divide a city into small areas, or cells. As a cell-phone user drives down the street, the signal is handed from tower to tower. A jamming device transmits on the same radio frequencies as the cell phone, disrupting the communication between the phone and the cell-phone base station in the tower. Cell Phone Jammer is an instrument to prevent cellular phone from receiving and transmitting the mobile signals to the base station. Mobile Cell Phone Jammer can block all kinds of mobile phone's ringing sound at all places such as church, mosque, library, Movie Theater and meeting room. You just buy it and just attach it at some place. And you will never hear the bell sound of mobile phone any more.

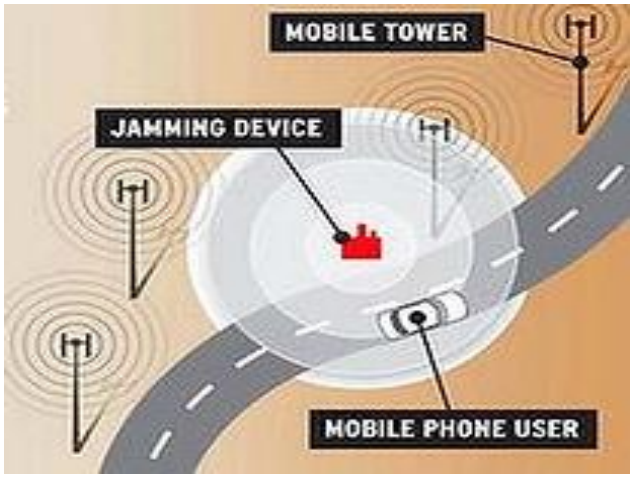

Fig2. Mobile Jamming.

C. Need & History of Jammers:

The rapid proliferation of cell phones at the beginning of the 21st century to near ubiquitous status eventually raised problems, such as their potential use to invade privacy or contribute to academic cheating. In addition, public backlash was growing against the disruption cell phones introduced in daily life. While older analog cell phones often suffered from poor reception and could even be disconnected by simple interference such as high frequency noise, increasingly sophisticated digital phones have led to more elaborate counters. Cell phone jamming devices are an alternative to more expensive measures against cell phones, such as Faraday cages, which are mostly suitable as built in protection for structures. They were originally developed for law enforcement and the military to interrupt communications by criminals and terrorists. Some were also designed to foil the use of certain remotely detonated explosives. The civilian applications were apparent, so over time many companies originally contracted to design jammers for government use switched over to sell these devices to private entities. Since then, there has been a slow but steady increase in their purchase and use, especially in major metropolitan areas.

As with other radio jamming, cell phone jammers block cell phone use by sending out radio waves along the same frequencies that cellular phones use. This causes enough interference with the communication between cell phones and towers to render the phones unusable. On most retail phones, the network would simply appear out of range. Most cell phones use different bands to send and receive communications from towers (called frequency division duplexing, FDD). Jammers can work by either disrupting phone to tower frequencies or tower to phone frequencies. Smaller handheld models block all bands from 800 MHz to 1900 MHz within a 30-foot range (9 meters). Small devices tend to use the former method, while larger more expensive models may interfere directly with the tower. The radius of cell phone jammers can range from a dozen feet for pocket models to kilometers for more dedicated units. The TRJ-89 jammer can block cellular communicat-ions for a 5-mile (8 km) radius.

Less energy is required to disrupt signal from tower to mobile phone than the signal from mobile phone to the tower (also called base station), because the base station is located at larger distance from the jammer than the mobile phone and that is why the signal from the tower is not as strong. Older jammers sometimes were limited to working on phones using only analog or older digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems (CDMA, iDEN, GSM, et al.) and are even very effective against newer phones which hop to different frequencies and systems when interfered with. As the dominant network technology and frequencies used for mobile phones vary worldwide, some work only in specific regions such as Europe or North America. Some Cell Phone Jammers have been introduced to some State Prisons in the United States. Cell phones that have been sneaked into prison pose a security risk for guards and property owners living nearby.

D. Problems in Existing Jammers:

The Common Problems are listed below:

- The person didn't even get the notification of a call or message when he is in the jammer coverage area.

- The person cannot be contacted for some urgent information also.
- Nearly the mobile phone will be in Switch Off state.
- There will not be any notification that the user mobile has been jammed.

III. PROPOSED MOBILE JAMMER DESIGN

In most countries, it is illegal for private citizens to jam cell-phone transmission, but some countries are allowing businesses and government organizations to install jammers in areas where cell-phone use is seen as a public nuisance. In December 2004, France legalized cell-phone jammers in movie theaters, concert halls and other places with performances. France is finalizing technology that will let calls to emergency services go through. India has installed jammers in parliament and some prisons. It has been reported that universities in Italy have adopted the technology to prevent cheating. Students were taking photos of tests with their camera phones and sending them to classmates.

A. Alternatives to Cell Phone Jamming

While the law clearly prohibits using a device to actively disrupt a cell-phone signal, there are no rules against passive cell-phone blocking. That means using things like wallpaper or building materials embedded with metal fragments to prevent cell-phone signals from reaching inside or outside the room. Some buildings have designs that block radio signals by accident due to thick concrete walls or a steel skeleton. Companies are working on devices that control a cell phone but do not "jam the signal." One device sends incoming calls to voicemail and blocks outgoing calls. The argument is that the phone still works, so it is technically not being jammed. It is a legal gray area that has not been ruled on by the FCC as of April 2005. Cell-phone alters are available that indicate the presence of a cell-phone signal. These have been used in hospitals where cell-phone signals could interfere with sensitive medical equipment. When a signal is detected, users are asked to turn off their phones. For a less technical solution, Caudal Partners, a design firm in Chicago, has launched the SHHH, the Society for Handheld Hushing. At its Web site, you can download a note to hand to people conducting annoying cell-phone conversations, expressing your lack of interest in what they're talking about

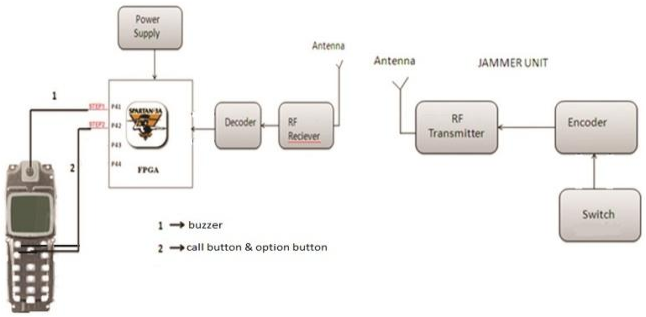

Fig3. Mobile Jammer General Diagram

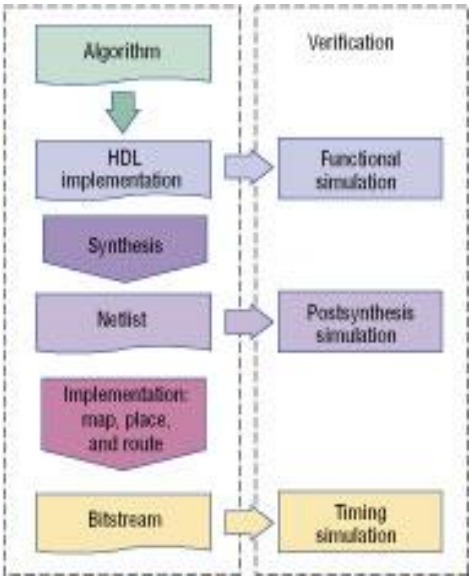

Fig4. Basic Flow Diagram of Fpga

IV. FPGA

Field programmable gate arrays (FPGAs) are emerging in many areas of high performance computing, either as tailor made signal processor, embedded algorithm implementation, systolic array, software accelerator or application specific architecture. FPGAs are so flexible and reconfigurable that they are capable of massively parallel operations, explicitly tailored to the problem at hand. There are lot of paradigms to put FPGAs at work in a high performance computing environment There are number of limitations which restrict FPGAs to reach the performance of Application Specific Integrated Circuits (ASICs) but they provide the possibility of changing the hardware design easily while outpacing software implementations on general purpose processors.

A. Basic Flow Diagram of FPGA

There are number of advantages using FPGAs including speed, reduced energy power consumption. As in reconfigurable computing, hardware circuit is optimized with the application so that the power consumption will tend to be much lower than that for a general-purpose processor. FPGAs have other advantages which comprised of reduction in size, component count (and hence cost), improved time-to-market and improved flexibility and extendibility. FPGAs offer tremendous performance potential. They can support in number of different parallel computation applications and implemented in single clock execution time. If FPGAs are reprogrammable then they can provide on chip facility for a number of applications. Due to the presence of on-chip memory facilitate co-processor logic's memory access bandwidth is not restricted to the number of I/O pins present in the devices. Moreover, memory is also closely coupled to the algorithm logic so therefore, no external high-speed memory cache is needed. And due to that power-consuming cache access and coherency problems can be avoided.

V. RF ENCODER AND DECODER

A. General Encoder and Decoder Operations:

The Holtek HT-12E IC encodes 12-bits of information and serially transmits this data on receipt of a Transmit Enable, or a LOW signal on pin-14 /TE. Pin-17 the D_OUT pin of the HT-12E serially transmits whatever data is available on pins 10,11,12 and 13, or D0,D1,D2 and D3. Data is transmitted at a frequency selected by the external oscillator resistor. By using the switches attached to the data pins on the HT-12E, as shown in the schematic, we can select the information in binary format to send to the receiver. The receiver section consists of the Ming RE-99 and the HT-12D decoder IC. The DATA_IN pin-14 of the HT-12D reads the 12-bit binary information sent by the HT-12E and then places this data on its output pins. Pins 10, 11, 12 and 13 are the data out pins of the HT-12D, D0, D1, D2 and D3.The HT-12D receives the 12-bit word and interprets the first 8-bits as address and the last 4-bits as data. Pins 1-8 of the HT-12E are the address pins. Using the address pins of the HT-12E, we can select different addresses for up to 256 receivers. The address is determined by setting pins 1-8 on the HT-12E to ground, or just leaving them open. The address selected on the HT-12E circuit must match the address selected on the HT-12D circuit (exactly), or the information will be ignored by the receiving circuit. When the received addresses from the encoder matches the decoders, the Valid Transmission pin-17 of the HT-12D will go HIGH to indicate that a valid transmission has been received and the 4-bits of data are latched to the data output pins, 10-13. The transistor circuit shown in the schematic will use the VT, or valid transmission pin to light the LED. When the VT pin goes HIGH it turns on the 2N2222 transistor which in turn delivers power to the LED providing a visual indication of a valid transmission reception.

B. Controlling the Project with a FPGA

Using these RF transmitter & receiver circuits with a FPGA would be simple. We can simply replace the switches used for selecting data on the HT-12E with the output pins of the FPGA. Also we can use another output pin to select TE, or transmit enable on the HT-12E. By taking pin-14 LOW we cause the transmitter section to transmit the data on pins 10-13. To receive information simply hook up the HT-12D output pins to the FPGA. The VT, or valid transmission pin of the HT-12D could signal the FPGA to grab the 4-bits of data from the data output pins. If you are using a FPGA with interrupt capabilities, use the VT pin to cause a jump to an interrupt vector and process the received data. The HT-12D data output pins will LATCH and remain in this state until another valid transmission is received.

NOTE: You will notice that in both schematics each of the Holtek chips have resistors attached to pins 15 and 16. These resistors must be the exact values shown in the schematic. These resistors set the internal oscillators of the HT-12E/HT-12D. It is recommended that you choose a 1% resistor for each of these resistors to ensure the correct circuit oscillation.

C. Range of Operation

The normal operating range using (only) the LOOP TRACE ANTENNA on the transmitter board is about 50 feet. By connecting a quarter wave antenna using 9.36 inches of 22 gauge wire to both circuits, you can extend this range to several hundred feet. Your actual range may vary due to your finished circuit design and environmental conditions.The transistors and diodes can be substituted with any common equivalent type. These will normally depend on the types and capacities of the particular loads you want to control and should be selected accordingly for your intended application.

D. RF Details

The TWS-434 and RWS-434 are extremely small, and are excellent for applications requiring short-range RF remote controls. The transmitter module is only 1/3 the size of a standard postage stamp, and can easily be placed inside a small plastic enclosure.TWS-434: The transmitter output is up to 8mW at 433.92MHz with a range of approximately 400 foot (open area) outdoors. Indoors, the range is approximately 200 foot, and will go through most walls.....

Fig5. RF 434MhzTransmitter. Modulation ASK

The TWS-434 transmitter accepts both linear and digital inputs, can operate from 1.5 to 12 Volts-DC, and makes building a miniature hand-held RF transmitter very easy. The TWS-434 is approximately the size of a standard postage stamp.

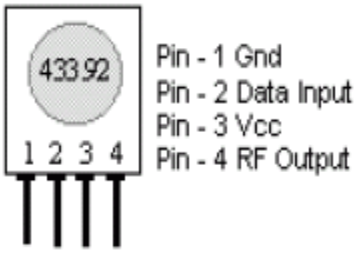

Fig6. RF-434 Pin Diagram

TWS-434RF Receiver operates at 433.92MHzFrequency and at Voltage: 4.5V~5.5V and Bit-rate: 0.2kbps-4kbps.

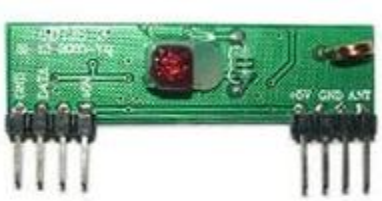

Fig7. RF Receiver

E. LCD Display

More FPGA devices are using 'smart LCD' displays to output visual information. The following discussion covers the connection of a **16x2 LCD display** to a PIC FPGA. LCD displays designed around Hitachi's LCD HD44780 module, are inexpensive, easy to use, and it is even possible to produce a readout using the 8 x 80 pixels of the display. Hitachi LCD displays have a standard ASCII set of characters plus Japanese, Greek and mathematical symbols.

Fig8. LCD Display.

F. LCD (Liquid Crystal Display) screen is an electronic display module and find a wide range of applications. A 16x2 LCD display is very basic module and is very commonly used in various devices and circuits. These modules are preferred over seven segments and other multi segment LEDs. The reasons being: LCDs are economical; easily programmable; have no limitation of displaying special & even custom characters.

VI. RESULT

A **16x2 LCD** means it can display 16 characters per line and there are 2 such lines. In this LCD each character is displayed in 5x7 pixel matrix. This LCD has two registers, namely, Command and Data. The command register stores the command instructions given to the LCD. A command is an instruction given to LCD to do a predefined task like initializing it, clearing its screen, setting the cursor position, controlling display etc. The data register stores the data to be displayed on the LCD. The data is the ASCII value of the character to be displayed on the LCD. Click to learn more about internal structure of a LCD.

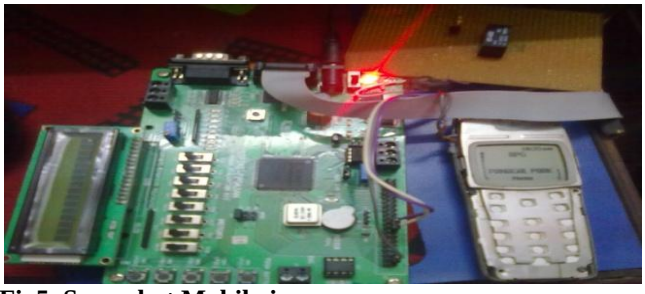

Fig5. Snap shot Mobile jammer.

VII. CONCLUSION

Our projected Mobile jammer is functioning utterly while not moving the signals from the network. In order that the user will able to get the notifications relating to Calls and messages (SMS, MMS). The notifications regarding the calls are given to the user. If there's any imperative decision as we will get the notification we will leave from the coverage space and use our mobile because it is. No would like of licensing. Implementation of our freshly designed jammers is straightforward. As we tend to square measure employing a FPGA, our hardware will be changed whenever we would like. FPGAs offer a number of paradigms to speed up calculations in a hardware software co-design environment. They are relatively cost-effective as compare to ASICs and due to flexible in nature, hardware resources are utilized in effective way.

VIII. REFERENCES

[1] SeongahJeong, Keonkook Lee, Heon Huh, and Joonhyuk Kang, "Secure Transmission in Downlink Cellular Network with a Cooperative Jammer," IEEE Wireless Communications Letters, Accepted For Publication, 2162-2337/13$31.00 _c 2013 IEEE.

[2]Y. Yang, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," IEEESignal Process. Lett., vol. 20, no. 1, pp. 35–38, Jan. 2013.

[3] M. Vzquez, A. Prez-Neira, and M. Lagunas, "Confidential communication in downlink beamforming," in Proc. 2012 IEEE Workshop on Sign.Proc. Adv. in Wireless Comm., pp. 349–353.

[4] S. Jeong, K. Lee, J. Kang, Y. Baek, and B. Koo, "Cooperative jammer design in cellular network with internal eavesdroppers," in Proc. 2012IEEE Mil. Comm. Conf., pp. 1–5.

[5] Q. Li and W. K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," IEEE Trans. SignalProcess., vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[6] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian
broadcast channels with common and confidential messages," IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5477–5487, Nov. 2010.

[7] R. Mochaourab and E. A. Jorswieck, "Optimal beamforming in interference networks with perfect local channel information," submitted to
IEEE Trans. Signal Process.Preprint available on arXiv:1004.4492, Oct. 2010.

[8] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "MIMO Gaussian broadcast channels with confidential and common messages," in Proc.IEEE Int. Symp. Inf. Theory, Austin, TX, Jun. 2010.

[9] E. Ekrem and S. Ulukus, "Gaussian MIMO broadcast channels with common and confidential messages," in Proc. IEEE Int. Symp. Inf.Theory, Austin, TX, Jun. 2010.

[10] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," IEEE Trans. Inf. Theory, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.
[11] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel," IEEE Trans. Inf. Theory, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

Author's Profile:

HAMEED MOHAMMED
Pursuing M.TECH in Very Large Scale Integration (VLSI) from Sri Indu College of Engineering & Technology.

.

V. PRATHYUSHA
Associative professor, Currently working in Sri Indu College of Engineering Technology in ECE dept.

K. Ashok Babu
Currently working as Professor & HOD, Dept of ECE in Sri Indu College of Engineering &Technology.