AN IMPLEMENTATION OF CYBER SECURITY FOR THE PROTECTION OF WOMEN

Mr.Enumula Mahesh[1] and Prof.Dr.M.Suman[2]

Abstract- An implementation of advanced high speed Encryption algorithmand image processing system is presented in this paper in order to improve the safety of the women data in terms of images in internet. The mathematic principle, encryption process and image processing are introduced. So as to reach the purpose of improving the system is to enhance security for images in the websites in order to reduce crimes and cyber bullying. The simulation results show that the advanced encryption algorithm implemented correctly. Using the method of encryption and image processing the data could be protected and authorized effectively.

Keywords: Encryption System, cyber bullying;

I. INTRODUCTION

With the development of Computer Network and Communication Technology, huge information and data need to exchange through communication channels and networks which are public. Safety of Data transmission becoming more and more important day by day with efficiency. The usage of internet becoming more day by day and it has become mandatory to upload everybody day including photographs.

These personal images leading to cybercrimes and cyber bullying especially in case of women. They are becoming victims of these crimes. This paper defining a security system which consists of an encryption algorithm and image processing system.

This provides the security for the images in the internet channels. Police can easily catch the criminals those who wrong practices with the images when the internet secured with this security system and eliminate further crimes.

II.CYBER BULLYING

Cyber bullying is the use of Information Technology to harm or harass other people in a deliberate, repeated, and hostile manner [1]. According to U.S. Legal Definitions, Cyber-bullying could be limited to posting rumors or gossips about a person in the internet bringing about hatred in other's minds or it may go to the extent of personally identifying [2]. The main aim of publishing materials is severe defaming or humiliating the targeted people or victims.

---

[1] *Department of Electronics and Communication Engineering KL University, Andhra Pradesh, India.*

[2] *Department of Electronics and Communication Engineering KL University, Andhra Pradesh, India.*

Nowadays with the advancement of technology, cyber bullying has become common in cyber world. Most of the cases are reported crimes against teenagers. High profile cases like the Suicide of Tyler Clement demonstrating the world cruelty of cyber bullying.

- Cyber bullying involves Impersonation, Exclusion.
- Cyber bullying commits Harassment, Cyber stalking, Denigration.
- Involves posting cruel rumors and creating falsehoods to damage reputation..
- Intentionally excluding someone from an online group in cruel acts.

Sometimes cyber bullying may be as simple as sending e-mails or text messages to harass someone who has denied further contact with the sender. It may include actions on public platforms such as social media with repeated threats like sexual remarks, derogatory labels for defamatory false allegations on a victim in order to make the person as a subject in online platforms for derision. It involves hacking into or deliberately destroys sites about a person, and posting false statements. The ultimate aim is to discredit or humiliate a targeted person. Cyber bullying may involves a single person or gang for targeting a single or a group or a community. It could be involved posting rumors about victim on the internet aims for bringing hatred in others minds in order to convince others to dislike or participate denigration of a target in online. It involves identifying personals of the victims and harm them by posting or publishing materials on public medium to severely defame and humiliate the victims.

Cyber bullies who are the culprits of cyber bullying discloses victims' personal data or information over public platforms. They discloses real name, home address, or workplace/schools of authenticated person at websites or forums by creating impression suck away that they are original. The process involves creating fake accounts, commenting, publishing material in their name etc. They targets victims for the purpose of defaming, discrediting.

In this process of cyber bullying it will become very difficult to catch offender by the cyber bully. Text chat or instant messages and email conversation among friends can also be cyberbullyfied. If the participants hurt with the what is said or displayed. They may use above content while committing the crime.

The recent advancements in technology and communication by using mobile applications in smart phones have accessibility of cyber bullying. It is expected that cyber bullying exclusive more with phones to a greater extent than other stationary internet platforms. The combination of cameras and Internet access instant availability through Smartphone technologies yield to specific types of cyber bullying which is not found in other stationary platforms. It is experienced a wider range of cyber bullying types through mobile phones than elsewhere.

IN SOCIAL MEDIA sites such as Facebook, Instagram and Twitter cyber bullying can take place. "By 2016, 90% of people bellow 18 are online. Youth spend more time with social media than any other activity." The cyber bullying is large risk attached with the social media. One million children were harassed, threatened or subjected to cyber bullying or other forms of cyber bullying on Facebook during the past few years. 90% of social media using teens have witnessed online cruelty while 35% have done this frequently. In Facebook there is a page dedicated to memory of guys who have lost their lives involved in the cruelty of cyber bullying. In most of the suicide cases they were bullied by creating them as homosexuals using their pictures.

III. IMPLEMENTATION OF SECURITY

Entire process consist of different steps first the IP address of the computer network which was user image was uploaded should be encrypted with encryption algorithm and to be processes with digital image processing this cannot be altered by any user only can accessed in the server. Image IP address can be retained from authenticated server system of the particular website.

A.   Encryption Principal:
This algorithm is based on finite field *GF* (28).The algorithm includes two mathematical operations: Multiplication and exclusive or, shown as formula[3].

$$\begin{cases} S_{0,c} = (\{02\} * S_{0,c}) \oplus (\{03\} * S_{1,c}) \oplus (\{01\} * S_{2,c}) \oplus (\{01\} * S_{3,c}) \\ S_{1,c} = (\{01\} * S_{0,c}) \oplus (\{02\} * S_{1,c}) \oplus (\{03\} * S_{2,c}) \oplus (\{01\} * S_{3,c}) \\ S_{2,c} = (\{01\} * S_{0,c}) \oplus (\{01\} * S_{1,c}) \oplus (\{02\} * S_{2,c}) \oplus (\{03\} * S_{3,c}) \\ S_{3,c} = (\{03\} * S_{0,c}) \oplus (\{01\} * S_{1,c}) \oplus (\{01\} * S_{2,c}) \oplus (\{02\} * S_{3,c}) \end{cases}$$

The algorithm has different keys with different length of 128 bits, 192 bits and 256 bits, shown as table Nk(4, 6 or 8)
stands for the key length which is number of the words in the key. The round number is determined by the length of the key. The relationship shown in the Table 1.

Table 1. Relationship between round number and key length

ES	Key Length	Group Size	Round Number
ES-128	4	4	10
ES-192	6	4	12
ES-256	8	4	14

Figure.1 showing the architecture of encryption algorithm in implementation boards like vertex, Spartan board
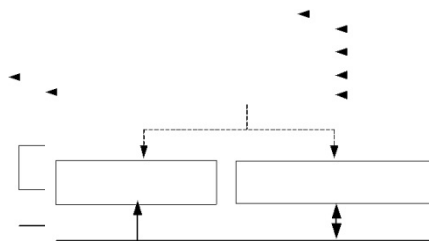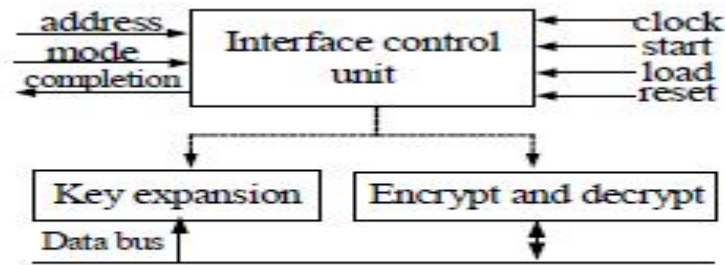
Figure 1.   module Architecture

B.   Encryption process:

Encryption process is an iterative group code with the Key. Theencryption process includes an initial key-addition called. AddRoundKey, then an initial round conversion for 1 r N times, finally a final round conversion again. All the roundconversions and initial key-addition make a state and a RoundKey as the input, and each cycle carries out four differentoperations to the Data flow, Sub Bytes, Shift Rows,Mix Columns and AddRoundKey. In order to accomplish anencryption process, ten times of round must be iterative. Figure 2 shows the flow of AES encryption algorithm[4][5].
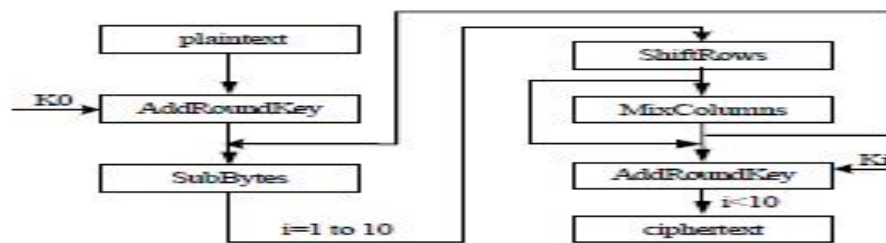

Figure 2.   Encryption algorithm flow

C. **Processing Image**:

The encrypted data i.e IP address of the
system will stored as the image header. This image header is a part of the image. IP address will be stored as the as image header while uploading image and will be modified after every modification in the network. This IP address is responsible for the image malpractices. This IP address can be accessed by only authenticated persons from the servers only[6][7].
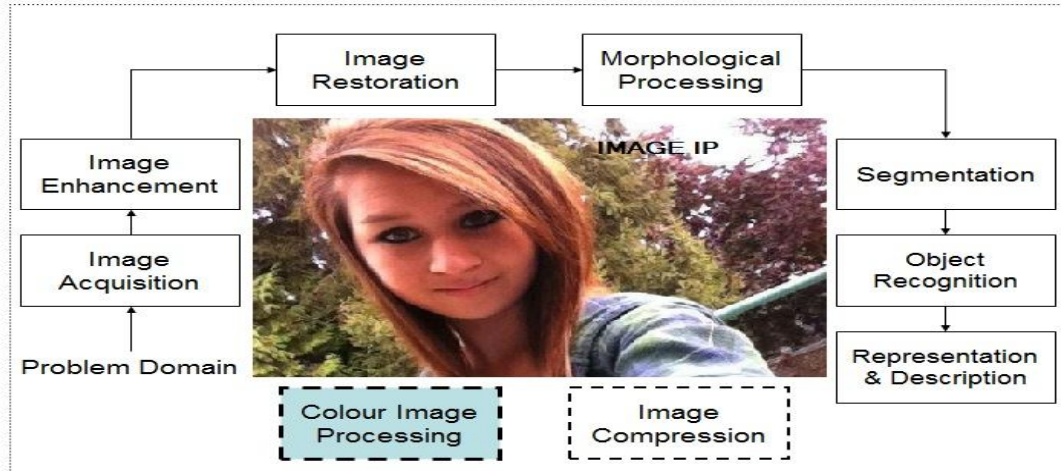
IV VERIFICATION AND CONCLUSION:

The design was tested in Xilinx Virtex-5 FPGA. The test result shows that the system could complete the whole process correctly in a 200MHz clock rate. Table.3 shows the worst path in timing analyzing report. The minimum period is 4.971ns[8].

Table 3. The report of the Timing constraint of the worst path in the system

Slack (setup path)	0.029ns
Source	Contrl/control_ps_FSM_FFd13
Destination	Data_reg_out_112(FF)
Requirement	5.000ns
Data Path Delay	4.812ns
Clock Path Skew	-0.124ns
Source Clock	Clk_BUFGP rising at 0.000ns
Destination Clock	Clk_BUFGP rising at 5.000ns
Clock Uncertainty	0.035ns
Total System Jitter	0.070ns
Total Input Jitter	0.000ns
Discrete Jitter	0.000ns

Plaintext: 27DABD46F9DA52D79967B7A0B33A492E
User_key: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
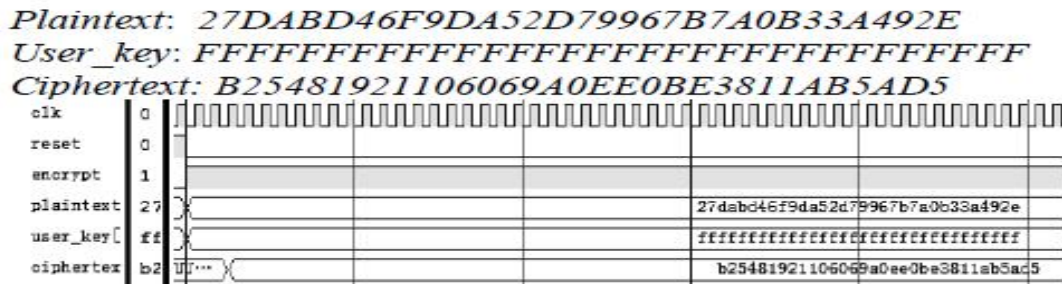*Ciphertext: B25481921106069A0EE0BE3811AB5AD5*

Figure 7. Decoding table and simulation result

REFERNCES

[1] "Legal Debate Swirls Over Charges in a Student's Suicide". *New York Times.*

[2] "Definition of Cyber-Bullying". *USLegal.com. US Legal, Inc*. Retrieved 5 February2016.

[3] "Zhenzhen Liu. Implementation of AES Encryption based on FPGA". Modern electronic technology, 2007,23(3),pp:103-104.

[4] "Jinxiang Shao. The high speed implementation of AES encryption algorithm based on FPGA". SichuanouthwestOil College, 2005.

[5]   "Ma Su,WangJi.High speed implementation of AES algorithm based onFPGA".The application of PLD/CPLD/FPGA, 1008-0570(2009)09-2-0127-02,pp:127-128.

[6] ShanxinQu, GuochuShou, YihongHu, ZhigangGuo, ZongjueQian. HighThroughput Pipelined Implementation of AES on FPGA. InternationalSymposium on Information Engineering and ElectronicCommerce.2009

[7] Jianghua Deng, Zhihua Hu, JipingNiu. The Implementation and reach of AES Algorithm. Microcomputer Applications, 21(7),2005.pp:58-59.

[8] TianYun,Xu-Wen-Bo,Hu Bin. Xilinx ISE Design Suite 10.xGuide.Posts&Telecom Press, Bei jing,2008.