AN INTELLIGENT EMBEDDED SYSTEM FOR PAY PHONES TO DETECT CYBER CRIMES

J. Nandini Meeraa[1], N.Indhuja[2], S. Devi Abirami[3] and K. Rathina Kumar[4]
[1, 2, 3]Department of CSE, Narasu's Sarathy Institute of Technology, Salem, India
[4]Department of ECE, Knowledge Institute of Technology, Salem, India

ABSTRACT

This paper proposes a mechanism which is used to provide security against the threats given to the patrols through the coin pay call access system. In this case the details of the person doing this offense is needed it can be obtained through this proposed system. This is executed using the image processing unit where the image and the biometric details of the person dialling the police station is captured and processed then it is sent to the networking unit and database unit where the image is compared with the nationalised database in the central processing unit using NIDR processor. The overall theme of this proposal is to build a system which can eliminate the illegal act of causing threatening by providing false information to the patrols. The challenge in this process is to develop the system by using the advanced techniques in the process gathering information and processing it to the control room if requested for the further investigations.

KEYWORDS: *Cybercrimes, Image processing, Networking Unit, Database unit & NIDR Processor*

I. INTRODUCTION

The importance of the implementation of this proposal, An Intelligent Embedded System for pay phones to reduce cybercrimes by using NIDR Processor lies basically on the usage of the coin pay call access system even in the present scenario. In-spite of various technologies being developed in the process of communication and there are lots of resources through which we can communicate with each other's, like mobile phones, Internet and there are also a lot of mediums being invented for the communication purpose like VOIP etc,. But the usage of the coin pay call access system is still dominant among the people throughout the world, mainly in the airports and commonly in the streets in many countries. Urge of developing this system was mainly due to the shocking statistical results of the threatening offence made through the coin pay call access systems to the patrols to give false information [1]. The main reason of designing this system for the coin pay call access system is because most of the threatening calls are made in order to provide an absurd occult information to the patrol is given through these system because it is very easy to escape and there is no much evidence so it is also difficult to indict the offensive person. This project is the ultimate solution of all this entire problems of creating blank call records to the patrols. The block diagram for the implementation of the system is very simple but at the same time the uses provided by it are abundant in both security management and the information retrieval process. This entire paper's main motive is to help the patrol in the above mentioned situation.

The core idea of this process is placing the micro camera as an in-built part of the coin pay call access system and enabling it to start its recording when a frequency of centralized patrol control number or the local patrol numbers is dialled. The captured image is processed and encrypted and compared with the database which is maintained nationally. Thus the complete information of the person calling to the patrols can be easily obtained if required by the officials. The process of placing a camera in a particular location or a medium to observe its action and ensuring security is a common system but

the architecture of the Intelligent Embedded System for pay phones to reduce cybercrimes by using NIDR Processor system completely gives the information of the offence being made through the coin pay call access system by retrieving full details of the offender by comparing the captured images with the nationalized database which will be maintained by each nation.

II. AN INTELLIGENT EMBEDDED SYSTEM FOR PAY PHONES TO DETECT CYBERCRIMES USING NIDR PROCESSOR

The illegal calls done from the coin pay call access system can be controlled by placing the micro camera and biometric sensor system in the pay phone system. The working of pay phone system will be clearly explained and understand by seeing the below figure 1.

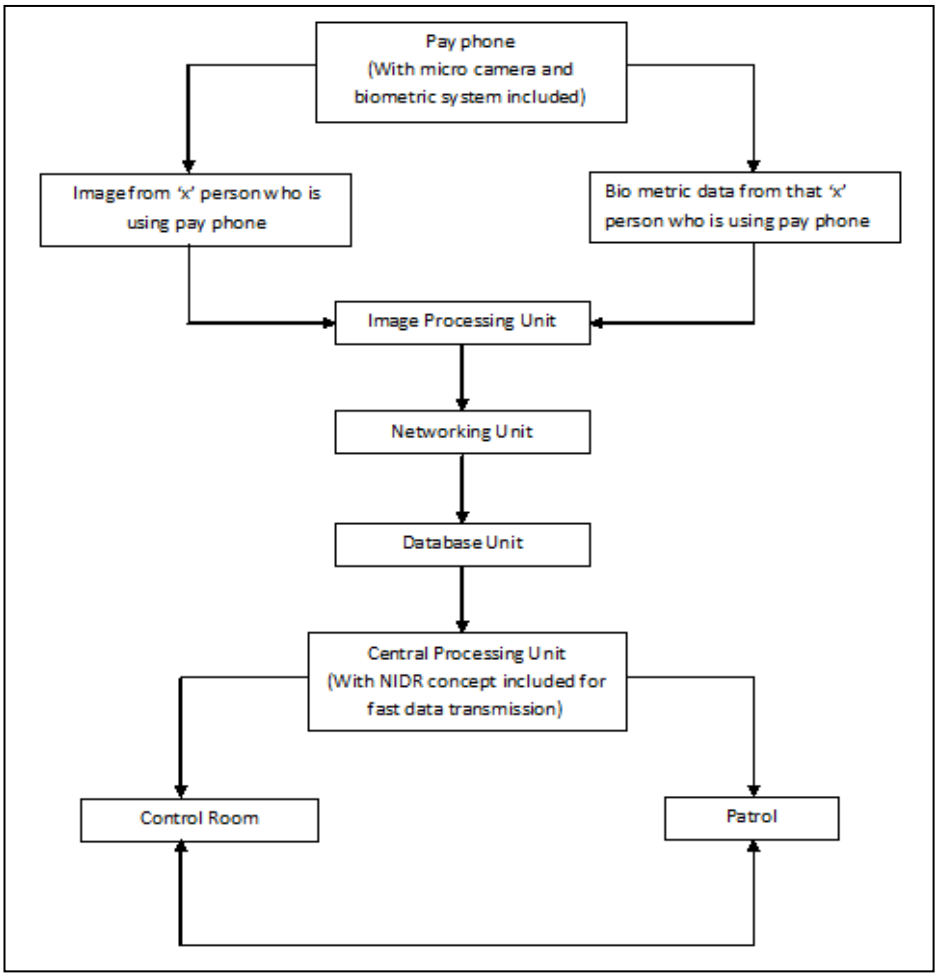

Figure 1. An Intelligent Embedded System for pay phones to reduce cybercrimes by using NIDR Processor

The coin pay call access system is very popular and it is being used all over the world. But the illegal calls done from the pay phone system is increasing day by day which leads to a huge problem and mainly the illegal calls are coming during the visit of the VIP's in that particular area, criminal take a chance to call the patrol and give a false threat or a rumour and distracting the policemen. To prevent this we are using the camera and the biometric observer system in the pay phone system. The working of the pay phone system starts when the person dials the number the particular frequency is traced and the system starts working immediately. The person's image and the fingers prints will be automatically captured using the camera and biometric system respectively. Both the image and the finger prints will be captured and it will send to the image processing unit. The image processing unit will perform many steps to convert the image into data and encrypt it and send it to the networking unit. The networking unit will be connected to the all patrols and control rooms. The networking unit

will be connected to the Database unit. The information in the networking unit will be send to the database unit. The database unit will contain the nationalised database which will have the name, address, gender, age, nationality, etc of the every individual person. So we can easily collect the full information about the particular person who is doing the illegal call from the pay phone using this system which is done in the central processing unit with the concept of NIDR [2].

III. IMAGE PROCESSING UNIT

Image processing is the process of giving the input as the image and getting the output as the image and parameters of the image. There many secured embedded video recorder in computing [2**].**

3.1. Image Acquisition

It is structuring the image in windows operating system it is a software used as a graphical interface that communicates with the image and the hardware devices like scanner, cameras etc. Image acquisition also supports push scanning and multi-image scanning.

3.2. Image Pre-processing

It is the process of enhancing the data image to computational process. The next step is Image preprocessing, accurate conditions such as shadows removing are noise elimination is done in image preprocessing [3]. BANCA and XM2VTS are the databases used in the face reorganization process.

3.3. Image Segmentation

It is the form of representing the digital image into multiple segments. Image segmentation is mainly used to locate objects and boundaries i.e.) lines and curves of an image. It will assign a label to each pixel. By using interpolation algorithm we can do 3D reconstruction.

3.4. Image Representation

It is the retrieval of image pixel and commonly they will represent set of pixels encoding the color and brightness in matrix format. Full image retrieval in a bitmap form is done by using contour representation.

3.5. Image Recognition

The next is the Image recognition, the recognition of the description part of the image which is being processed is carried out [4]. When it is match with the database it will know what is on the original picture.

3.6. Image Interpretation

It is the process of identifying the significant of the image i.e.) the shape, size, shadow, texture and pattern.

3.7. Final Module of Image Processing Unit-Cryptography

The image which being processed has to transmitted safely. Cryptography is the process of making a secured communication or transmission and the techniques used in cryptography are data integrity, data confidentiality and authentication. The techniques used in the process of cryptography are explained as follows.

ENCRYPTION AND DECRYPTION: Encryption is the process of changing plain text into cipher text. It is mainly used to secure the data from the third party. Decryption is the process of making cipher text to plain text. There are three algorithms mainly used in cryptography they are secret key cryptography, public key cryptography and hash function. Here we choose the simple cipher to the encryption process.

VISUAL IMAGE CRYPTOGRAPHY: The image is securely transmitted by some steps followed first it will change the image input to binary form then into half tone image by density of dots formed by the gray color image then the image become transparent then the image is decrypted then it follows the same steps to encrypt the image [5].

IV. NETWORKING UNIT

After the image processing unit next the data is encrypted and sent to the networking unit where the it is decrypted to the original data, it is done to maintain security while the transmission process. In the networking unit the different types of the data of the image being acquired from the person are being collected and the networking of the details and information of the offender is carried out here. The information such as the image of the person and the biometric details are combined in order to get accurate data of the person. Importance is given to this unit because when the data are networked the speed of the further processing can be done and the correctness of the information can be kept in account. After which this will be taken to the database unit.

V. DATABASE UNIT

In the database unit will a nationalized database in it. Nationalized database is a database which will be maintained by every nation or a country. It will have details about each and every citizen of the country. This database will have the name, photo, address, age, birth of date and also may include the biometric details like finger prints etc. The process which will be done on the database unit is the comparison of the data of the offender which we have collected so far. It will have the image of the person and few biometric details which will be compared with the nationalized database and if the image matches the address of the person will be immediately retrieved and taken for further investigation if needed by the patrol. The output is taken to the central processing unit which is explained as follows.

VI. CENTRAL PROCESSING UNIT

Once the frequency of 100 is dialled from the coin pay call access system the micro camera being present in the system is activated automatically and captures the image and the biometric data of the person is being captured. The captured image is sent to the image processing unit where the image is converted into data. This data will be now transmitted for the further processing. In-order to maintain security of the data while transmission and processing the data has to be encrypted undergoing the cryptography process. The network unit integrates all sorts of details of the person such as the image and the biometric details forming the complete analysis of the person with full information as possible. Next the comparison is done with the nationalized database and the accurate information and the details are gathered. Finally this data is carried to the central processing unit where the processed information will be maintained and transmitted if required by the patrol and the control room.

The central processing unit is the core of the Intelligent Embedded System for pay phones to reduce cybercrimes by using NIDR Processor. Here we use the NIDR processor for the central processing unit because of many advantages of it over other processors [7]. The main advancement in the NIDR processor which is the Nurture IDR segmentation and multiple instruction queues in superscalar pipelining processor is the pipelining unit in which the fetched and the type of the instruction is being identified and then send to multiple instruction queues based on its types [6]. The decoding of the

instructions is done separately for each type forming multiple decoding units. Similarly the executions of the instructions are also done in multiple units and the output is written by combing the results from all the units.

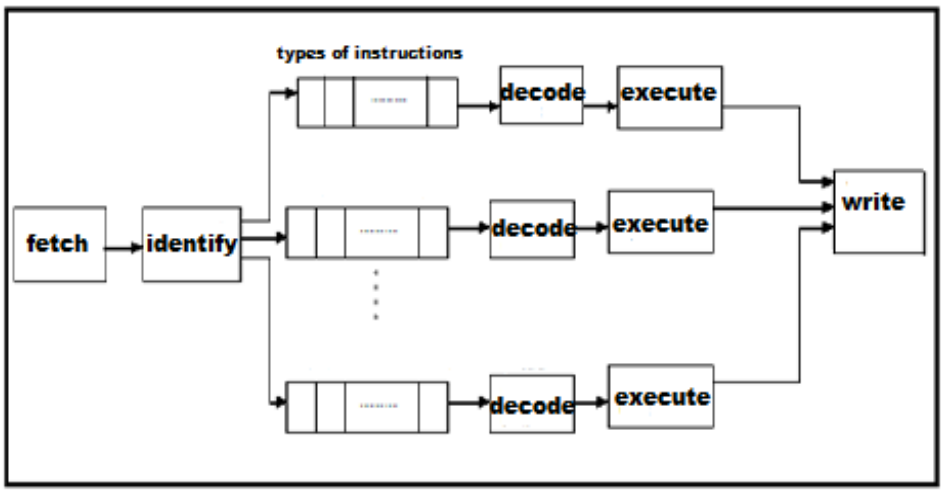

Figure 2. NIDR Processor

From the working of the Nurture IDR segmentation and multiple instruction queues in superscalar pipelining processor we can achieve more speed and accurate output in all the types of the instruction that we carry out through this than the other processors [8]. This processor can make the Intelligent Embedded System for pay phones to reduce cybercrimes by using NIDR Processor, sustain in all types of the environments where it will be implemented. We can surely experience a fast data transmission of the data and information by using the NIDR processor in built central processing unit. The gather information of the person doing the crime of producing false information or the threats to the patrols can be identified completely so that the work load of the officials can be reduced through a computerized mechanism. If the patrol is in need of the person they can contact the control room and the data of the person can be sent to and from the control room patrols and the central processing unit. All the request and processing response to the received request will be handled by the central processing. The maintenance of the information being stored in the central processing are also managed perfectly in case of future use.

As discussed earlier the statics survey of the crime of providing occult information to the patrols to distract the policemen is the main reason which made us to develop this kind of the system to identify the offender. We take real pride and happiness in designing the Intelligent Embedded System for pay phones to reduce cybercrimes by using NIDR Processor system which will help the policemen who are striving and working hard to protect and provide security to people in different parts of all over the world. Hope this system will definitely help the patrol in tracing out criminals who do the cheap job of creating false threats to the policemen by disturbing and diverting them from their work. The accuracy of this system will be promising and the speed will also be very high. The formulation and the implementation of this system are very cost effective so that it can be used throughout the world. The benefits of using this concept and the system will be remarkable. This implementation of this system can stop the use of coin pay call access system to do blank calls and give false threats so that the offender doing this crime from the coin pay call access system can escape easily without any identity proofs. All the working blocks involved in the implementation process are clearly explained and the functioning of the system is also elaborated in detail. The benefits of the Intelligent Embedded System for pay phones to reduce cybercrimes by using NIDR Processor are plenty so that it is recommended to the implemented and used all over the world.

VII. IMPLEMENTATION RESULTS

The implementation of the central processing unit work is done in order to evaluate the performance of this system. The job of the central processing unit is the core of this system where the processed image from the image processing is received and it has to compared unit the nationalised database and

the details of the offender has to be found. This process is implemented using Net Beans which is an IDE and language used is Java. To start this process first the software asks for the login which is shown in the figure 5 where the officials has to login with their username and password. Next step will be giving the input as the input for the system which is shown in the figure 4.

Figure 3. Login page of the system.

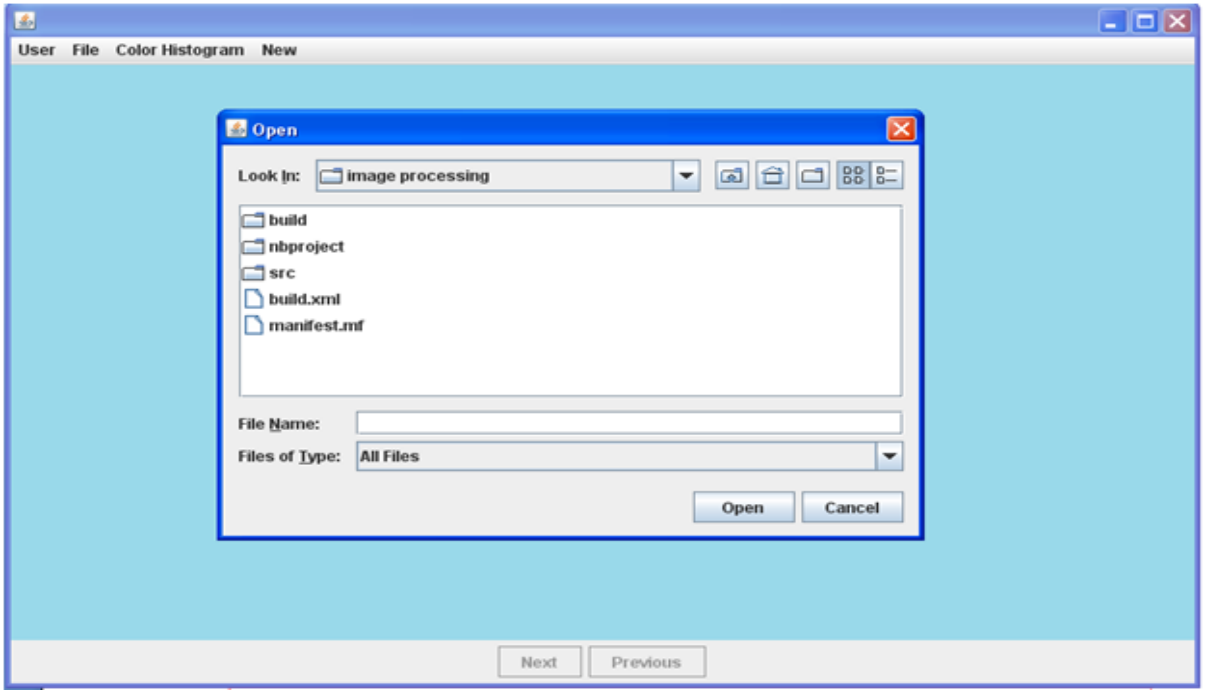

Figure 4. Setup for adding the source image file.

The step is once the image is given as the inputs as shown in the figure 5, to the system the search process will take place the image of the person will be compared will the nationalised database and so the biometric information like finger prints is also taken for the comparison process. Here we implemented this by using a sample image which is compared with the few details form of few people for example. After the image is given it split into different portions and we use the Content Based Image Retrieval technique where the split portions are taken as content and the search process begins. This system has few thousands of the fields stored in the database and it takes a time of 2188ms.

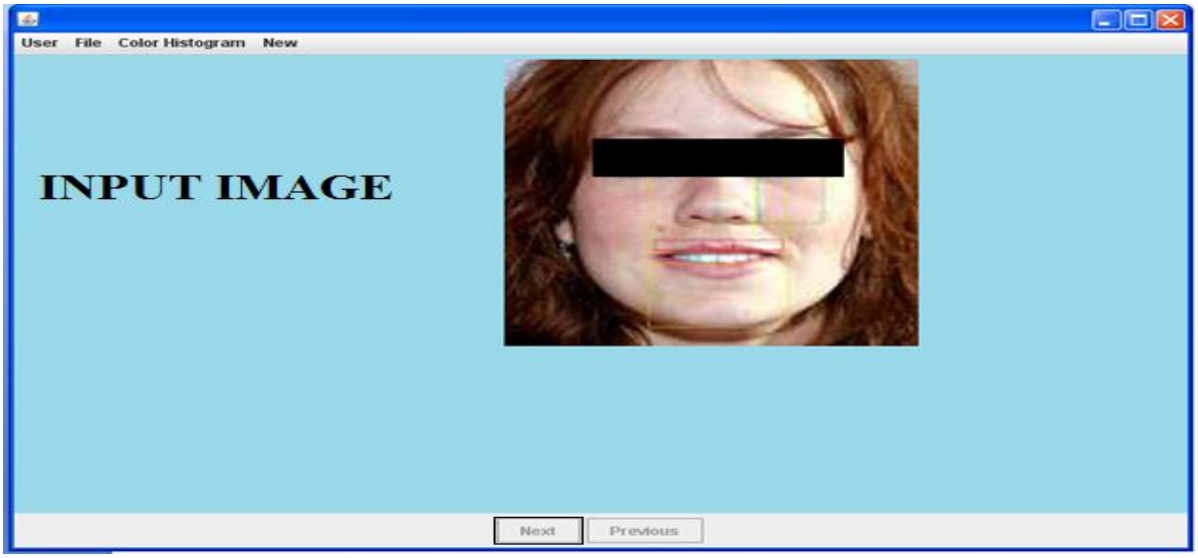

Figure 5. The image is given as the input to the system.

The final results will the process of retrieving the details of the offender from the nationalised database. The details such as the name, address, age, phone and the other details which will be usually present in the nationalised database is obtained so the offender is easily be acquiesced.

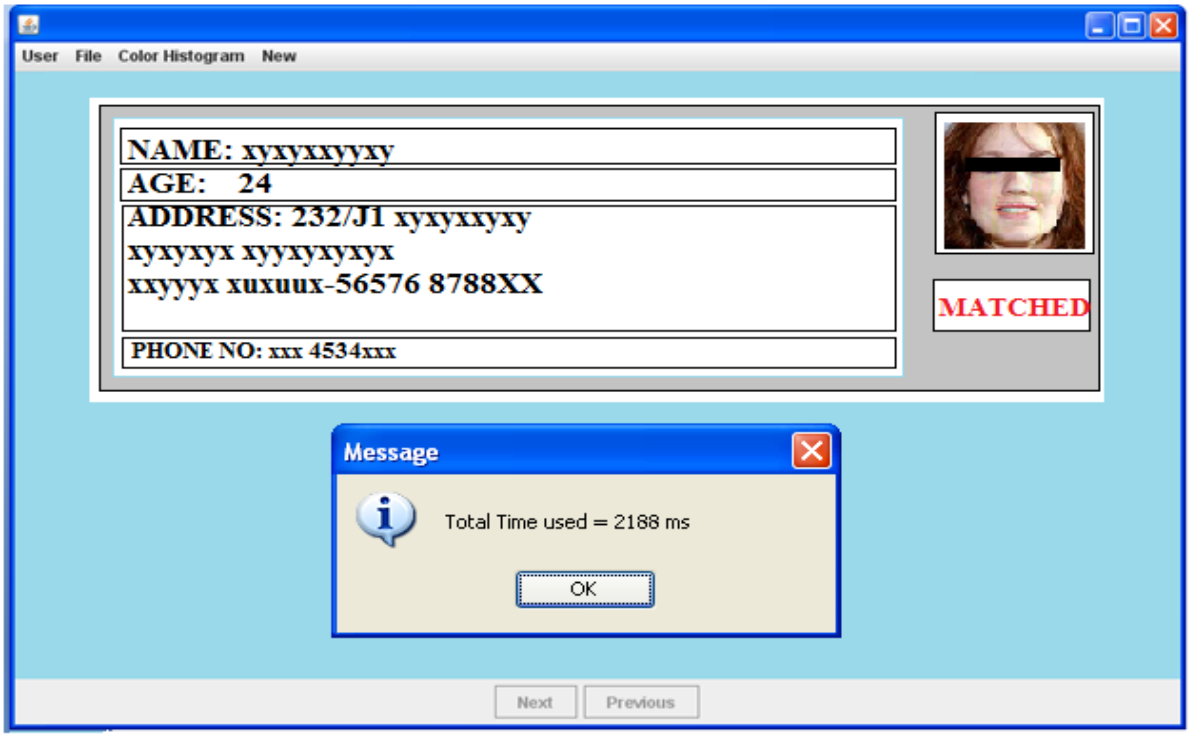

Figure 6. Results and the operation time.

VIII. RESULTS DISCUSSION

The result and the implementation of this system are tried with the database with few thousand of the fields of data. The captured image from the image processing unit reaches the database unit and the central processing unit where the image is compared with the nationalised database and if the image matches the results can be found easily. The important technique which is used here is the Content Based Image Retrieval so that even if the full face if the person cannot be captured by the camera in the pay phone the captured parts like the eyes or nose and even the biometric information can be used for the processing. The normal time consumption of this implemented system is calculated to be

2188ms which is reasonably fast than manually finding the offender. The above explained screen shots clearly shows the process which starts with the login and ends up by finding the offenders details from the nationalised database. The results are measured by the calculation of the operation time which directly shows the performance of the system. The sizes of the database can vary based the nation or the country which is using this system but the performances remains standard.

IX. CONCLUSIONS AND FUTURE SCOPE

An Intelligent Embedded System for pay phones to reduce cybercrimes by using NIDR Processor to help the patrol working to provide security to each of us. The rate of the offence that are taking place by using the coin pay call access system is extremely high than compared to other resource. So we hope that this model can be used by any nation to eradicate this crime. This paper has ultimately focused on the goal of creating a system which provides a solution against the offense of creating threats to the nation's patrols by giving false information. The various units and the techniques involved in this process are very advanced and efficient. We strongly trust that the threatening to the patrols taking place through coin pay call access must meet an end through this Intelligent Embedded System for pay phones to reduce cybercrimes by using NIDR Processor. This major effort we have into design is to make this system a very cost efficient one at the same time including very advanced and reliable operating units. A serious effort has been taken by us in the process of selecting the devices and the techniques involved in each unit of the system to make it a successful one.

REFERENCES

[1]. J.Nandini meeraa, S.Devi Abirami and K.Rathina Kumar, "Fast data transmission by cryptographically embedded system to avoid cybercrimes using NIDR" on International Conference on Computing Techniques, Embedded Systems and Drives at at PPG Institute of Technology, India on 7-9th March 2012.

[2]. ThomasWinkler and Bernhard Rinner, "Securing Embedded Smart Cameras with Trusted Computing", Hindawi Publishing Corporation EURASIP Journal on Wireless Communications and Networking Volume 2011, Article ID 530354, 2010.

[3]. A. Georgopoulos, A. Loizos,A. Flouda, "Digital image processing as a tool for pavement distress evaluation", ISPRS Journal of Photogrammetry and Remote Sensing,Volume 50, Issue 1, February 1995.

[4]. Richard J Prokop, Anthony P Reeves, "A survey of moment-based techniques for unoccluded object representation and recognition", CVGIP: Graphical Models and Image Processing Volume 54, Issue 5, 1992.

[5]. Morampudi Naresh Kumar, Datrika Srinivas Rao, D.Sravanthi, "A Noval Approach for Cheating Prevention through Visual Cryptographic Analysis", International Journal of Computer Science&Engineering Survey (IJCSES), Vol.2,No.4, November 2011.

[6]. R.Aravind, R.Lavanya and M.Senthil Kumar, "The Computerized Pen Drive" , IJCA International Journal of Computer Applications (0975 – 8887), Volume 41– No.5, March 2012.

[7]. R.Aravind, E.Jothinimal and J.Nandini Meeraa, "Data Exchange through digital and computerized USB device with security key", International conference on advanced technologies for research and product development by the department of Electronics and Communication Engineering at Kathir college of engineering, India.3-9-2012.

[8]. J.Nandini Meeraa, N.Indhuja, S.Devi Abirami and K.Rathinakumar, "Nurture IDR Segmentation and Multiple Instruction Queues in Superscalar Pipelining Processor", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.

AUTHORS

J. Nandini Meeraa pursuing bachelor's degree in computer science and engineering final year at Narasu's Sarathy Institute of Technology, Salem. Approved by All India Council for Technical Education, New Delhi (AICTE) and is affiliated to Anna University Chennai. I am a member of CSI computer society. My current research interest is on creating evolution in the speed of the processor. Published a research paper "Nurture IDR segmentation and multiple instruction queues in superscalar pipelining processor", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011 ISSN : 1694-0814. IF: 0.24. I

have presented a paper in National level conference on the title "Finest spot detection in spatial database using query processing" at Selvam College of Engineering on 17th February 2012 conducted by Department of CSE & IT & MCA on National Conference on Information Computational Algorithms and their Applications. Presented a paper in International level conference on the title "Fast data transmission by cryptographically embedded system to avoid cybercrimes using NIDR" at PPG Institute of Technology on 7-9th March 2012, Conducted by the departments of ECE & EEE on International Conference on Computing Techniques, Embedded Systems and Drives. Presented a paper, "Digitalized and computerized USB device with security key enabled" at the International Conference 'ICATRPD-2012' held at Karthir college of Engineering on 3rd September, Coimbatore. Presented a paper, "Applications of NIDR processor in embedded system and VLSI designed USB device" at the National conference 'NCRTAC12'held at SNS college on 5th October.

N. Indhuja is presently doing her final year B.E. specialized in Computer Science from Narasu's Sarathy Institute of Technology Anna University Chennai. She has published the journal on the topic "Nurture IDR Segmentation and Multiple Instruction Queues in Superscalar Pipelining Processor", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.She has presented a National level conference in Performance Analysis and Synthesis of Online Error Detection And Bits using AES Encryption Algorithm in 2012.

S. Devi Abirami is presently doing her final year B.E. specialized in Computer Science from Narasu's Sarathy Institute of Technology Anna University Chennai. She has published the journal on the topic "Nurture IDR Segmentation and Multiple Instruction Queues in Superscalar Pipelining Processor", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.She has presented a National level conference in Performance Analysis and Synthesis of Online Error Detection And Bits using AES Encryption Algorithm in 2012.

K. Rathina Kumar is presently assistant professor at Knowledge Institute of Technology, Anna University, Chennai. He has presented a paper in an International level conference in "Fast data transmission by cryptographically embedded system to avoid cybercrimes using NIDR" at Embedded Systems and Drives at at PPG Institute of Technology, India on 7-9th March 2012. "Nurture IDR Segmentation and Multiple Instruction Queues in Superscalar Pipelining Processor", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011. Published paper in the international journal in the title of "Efficient method for escalating the performance of programmable router for network on chip by lightweight circuit switched approach" in International Journal of Communication, Computation and Innovation[IJCSI] of volume 1, issue 2(Jan-July 2011) of ISSN 2229-6808; published paper in the international journal in the title of "Multi Machine power system stabilizer design using particle swarm optimization technique" in International Journal of Communication ,Computation and innovation[IJCSI] of volume 1, issue 2(Jan-July 2011) of ISSN 2229-6808; Presented a paper in National level conference on significant challenges of smart antennas in ADHOC networks at Idhaya Engineering College on 26th March 2011 conducted by department of CSE, ECE & IT in the title of National Conference on Advanced Computing and Communication Systems; Presented a paper in International level conference on channel noise cancellation using blind adaptive equalization at SSM college of engineering between September 21-23, 2011 conducted by Department of ECE in the title of International conference on Computer Communication & Signal Processing (IC3SP)-2011;