IOP Conf. Series: Materials Science and Engineering **263** (2017) 052040 doi:10.1088/1757-899X/263/5/052040

Smart security and securing data through watermarking

Ritesh Singh, Lalit Kumar, Debraj Banik and S Sundar
School of Electronics Engineering, VIT University, Vellore 632014, Tamil Nadu, India

E-mail: sundar.s@vit.ac.in

Abstract. The growth of image processing in embedded system has provided the boon of enhancing the security in various sectors. This lead to the developing of various protective strategies, which will be needed by private or public sectors for cyber security purposes. So, we have developed a method which uses digital water marking and locking mechanism for the protection of any closed premises. This paper describes a contemporary system based on user name, user id, password and encryption technique which can be placed in banks, protected offices to beef the security up. The burglary can be abated substantially by using a proactive safety structure. In this proposed framework, we are using water-marking in spatial domain to encode and decode the image and PIR(Passive Infrared Sensor) sensor to detect the existence of person in any close area.

1. Introduction

The word processing in today's world has two different types: Analog and Digital. Both has some advantages over one another. Digital processing is swiftly increasing for different applications in research areas of electronics and computer engineering technologies[1]. The possible methods involve image visualization, photo restoration, and watermarking for security purpose. Image refining using digital watermarking can be used for different purposes like filtering redundant noises from photos, image classification etc. The mainframe is representation of dimensional images using finite points of digital values named pixels [2]. In this paper, we are discussing the basic possibilities of obtaining protection of areas which be of utmost importance using digital water-marking techniques.

Now-a-days privacy and security is an important concern to everywhere. To overcome these challenge, we are going to propose a model to secure the precious or confidential treasure. In current scenario, there are many protection set-ups which contain CCTV (Closed Circuit Television) which continuously capture the video and lead to wastage of memory and do not provide much functionality, so to tame this issue we are presenting an idea with additional functionality of safety. We are using PIR sensor to detect the existence of any individuals. If any person tries to enter in room would come under the

range of PIR sensor, the photo of that person will be clicked and then for entering in the room he/she must enter the user name and password. If it would be correct, the gate will be opened to let the person enter. If the entered information is wrong, then the clicked photo will be sent to the control room for taking the respective action against the intruder. Here the photo will be encoded using the method of image processing i.e. Water-marking. By this process we will hide the image into a cover image and then it will be transmitted to the nearest police station or concern department. Photo will be encoded so that no one can hack the photo. At the receiver side, the photo will be decoded and appropriate action will be taken immediately.

2. Methodology

Digital image processing deals with the manipulation of digital images through a digital computer. It is a sub field of digital signal processing but focus particularly on images.Watermarking is a part of digital image processing. It is a process in which image or text is embedded into another image which can be visible or invisible.

Two types of watermarking can be done.

- Visible watermarking
- Invisible watermarking

If the information image can be seen in the watermarked image then it is called visible watermarking. If information image cannot be seen in the watermarked image i.e. in hidden form then it is called invisible watermarking. In this paper, we are going to use invisible watermarking for cyber security purpose.

In our system, we are using P.I.R sensor, a camera, a relay and R-PI 3.We are using Passive infrared sensor to click the photo via camera. Whenever a person would try to enter the room in the range of PIR sensor (120 degree), then the photo will be clicked by the camera. Hereafter person has need to enter the user id and password. if entered id and password will be correct the gate will be opened so that the person can enter to that place. Total three chances will be given to the user. Every time user friendly massage will be displayed that 'You have two or one chances to enter correct id and password'. If he/she entered a wrong-id at the first or second attempt a message will be come on the screen which will tell that how many chances has been remained. User entered wrong id and password in all the three attempt the photo will be clicked and it will be sent to the control room. Up to, that much will be done by the raspberry Pi and sensor. We have added on the raspberry Pi with the MATLAB and coding will be done in the MATLAB only.

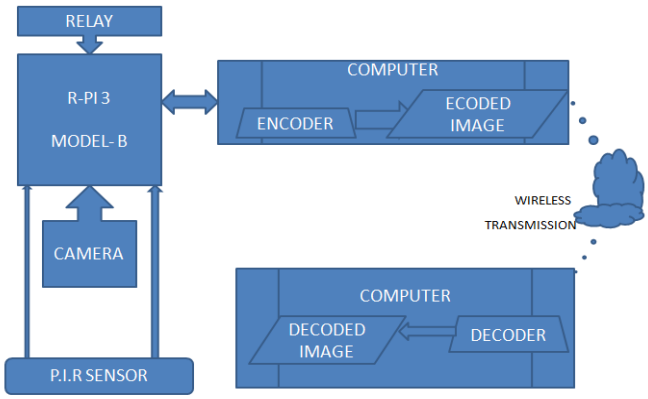

Figure 1. Block Diagram.

The clicked photo will be saved in the database. After that the image will be encoded before being sent to the concerned place or the person to prevent the any kind of mislead before being taken of any action. This encoding is done by invisible watermarking. It is done by LSB (Least SignificantBits) watermarking. We know the maximum information of photo is kept in the msb bit of pixel compare to the LSB. So here we will manipulate the pixels of LSBwith MSB (Most Significant Bits). During encoding we will take two image inputs, one is cover image and another one is information image i.e. the clicked image. In the processing unit, we will replace the LSB bit of cover image by the MSB bit of information image. At the output of encryption, we will get the single image that is watermarked image, which is caring the MSB bit of information image as its LSB bits. So, if anyone hack the image he will get that un-useful cover image[3]. It was the purpose of encoding. The watermarked image will be sent to the concern sector. After receiving that picture at destination here it can be decoded to get the image of intruder. That is done by reverse way of encoding i.e. separating the MSB and LSB bits of cover image and information image. At the output, we get the information image. We can recover most of the information, henceforth no loss will be there.

2.1 Components

(a) SOFTWARE

MATLAB: The photo whatever has been sent by the Ri-pi it will be received in the MATLAB.At the receiver end it will encypt the image or at the destination side it will be decrypted.

(b) HARDWARE

- *CAMERA*: It will click the photo of the person, who would come under the range of PIR sensor.
- *R-Pi 3 (MODEL-B):* It will transmit the clicked photo to MATLAB for encoding and decryption purpose.
- *P.I.R. SENSOR*: For Continuously Monitoring the area.
- *RELAY*: For opening and closing of premises.
- *Display with Keyboard:* For entering the userid and password.

2.2 Algorithm

Encoder:
Input: Cover Image
Output: Watermarked Image
Step 1: i← cover image
j← information image
Step 2: i= i*2; (Doubling size of cover image)
Step 3: j ← j AND Msb;
Step 4: j ← j left-shift to Lsb;
Step 5: for k ← 1 to j
r ← i BITOR j;
Step 6: Store r ← Watermarked Image

Decoder:
Input: Watermarked Image
Output: Cover Image and Information Image

Step 1: r ← Watermarked Image
Step 2: r ← r /2;
Step 3: for i ← 1 to r
j ← j BITAND r;
k ← k BITOR r;
Step 4: j ← j right-shift to Msb;
Step 5: Display both k and r corresponding to Information and Cover Image

3. Results and Discussions

In the model, the camera monitoring the area capture the photo sent by the R-Pi as soon as the person comes in the range of sensor. The information captured by the camera is send to the MATLAB environment for further process.

The MATLAB code will check the password criteria and does the further part of encoding in steps. First it will ask the cover image to be inserted and then the information image i.e. person image to be encapsulated. The output of the encoder i.e. watermarked image and the output of the decoder i.e. information image is given below:

Figure 2..Encoder output (Watermarked Image)

Figure 3. Decoder output (Information Image)

4. Conclusion

In our projected system, currently we are using only id and password matching system but for making the security two tier image comparison (with the pre-defined database) feature in machine learning can also be added. The advantage of this feature is that suppose any unauthorized person any how come to know the correct information, whatever is required to enter, he/she will be caught by this feature. As far as the watermarking is concern recently we are using in spatial domain later it can be used in frequency domain which would be more secured as compared to it alternative.

The smart security system using water marking is implemented. It is more secured and cost effective as well [4].This system significantly contributes to situation monitoring. Our system senses the intrusion and it send the notification to the respective person for any action being taken. It provides the following advantages:

- It saves the memory.
- Immediate action.
- The action can be taken during the attacks rather the action being done.

References

[1] Patel, P. B., Choksi, V. M., Jadhav, S., and Potdar, M. B. 2016 *Smart Motion Detection System using Raspberry Pi Foundation of Computer Science FCS* **10** 5.

[2] Nguyen, H. Q., Loan, T. T. K., Mao, B. D., and Huh, E. N. 2015 Low cost real-time system monitoring using Raspberry Pi *Proc. of IEEE International Conference on Ubiquitous and Future Networks (ICUFN)* 857-859

[3] Yahya, A.N., Jalab, H.A., Wahid, A. and Noor, R.M., *2015* Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network *Journal of King Saud University-Computer and Information Sciences*, **27** 4 393-401.

[4] Laouamer, Lamri, Muath AL Shaikh, Laurent Nana, and Anca Chrisitine Pascu. 2015 Robust watermarking scheme and tamper detection based on threshold versus intensity *Journal of Innovation in Digital Ecosystems* **2** 1 1-12.