IJCRT.ORG ISSN : 2320-2882
INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

INVISIBLE FENCING WITH HIDDEN WATCHDOG

[1]Mudem.BhavyaSri, [2]Mamidi.Pallavi, [3]Dr.Yerraboina.Sreenivasulu, [4]Manukonda.Rakesh

[12] Student, [3]Professor, [4]Assistant Professor
[1234]Electronics and Communication Engineering
[1234]Sreenidhi Institute of Science and Technology , Ghatkesar, Hyderabad, Telanagana, India

Abstract:

This project aims to put a cutting-edge home protection system within the grasp of the general population. Nowadays, theft from safe houses is common because thieves can get away with it easily. This plan was therefore developed to stop crimes like this. incorporate a stealth monitor into the plan. The speech chip will then instantly broadcast the audio message. The main concept behind the system is that the IR sensors will detect a passing individual from any of the four directions.

The concept is to successively trigger the magnetic switches using a permanent magnet. Magnetic controls placed behind the wall are concealed from view. The switch will be activated by a magnet put near it. These toggles can be positioned wherever the creator pleases. Only those with the necessary permission are aware of where these valves are located precisely. The right switches must be turned on in the proper symbolic sequence in order for the door to unlock. If the incorrect sequence is input three times in a succession, the door will stay closed and an SMS will be sent to the authorised mobile specified in the controller programme via the GSM interfaced to the controller.

A servo motor-driven sliding door mechanism is a component of the display section. A wooden plank is used to depict the wall that houses the entrance mechanism. Due to GSM's worldwide network and unrestricted range, users can receive communications wherever they happen to be. Also kept a mystery are the sites of the invisible magnetic controls.

KEYWORDS: IR sensors, Magnetic switches, GSM module, 33A3 voice module, H bridge

I. Introduction

Safety comes first in an Ambient Intelligent environment. Cryptographic algorithms as well as safe techniques for creating and keeping hidden keys are necessary in this situation. They are used for this purpose because they already have security features built in, such as being impossible to clone and leaving obvious indications of meddling. Both a security and a private precaution, the door will never unlock for anyone who isn't authorised. It is possible to put automated entrances that require a secret code in strategic areas where security is of the greatest importance. Consider private labs, safe vaults, etc. A normal component of many contemporary security methods is password protection. Here's an endeavour or strategy that enables you to accomplish more.

It is build with a strong security infrastructure that can be used by many different companies in addition to regular household purposes. Nowadays, theft from safe houses is common because thieves can get away with it easily. In order to prevent such robberies, this initiative has a built-in guard dog. The speech chip will instantly broadcast the audio message after the IR sensors detect a passing person, which is the system's main working principle.

In some places, users can use a swipe card or an RFID card to demonstrate their IDs. These techniques, however, are now outdated, so this project is intended to thrill participants as they crack the code using concealed devices placed inside the wall.

Electronic components are positioned to infiltrate every aspect of our lives as a result of their declining cost, decreasing size, and rising power. A network will link the electronics, and they will fit in with the environment. The gadgets are anticipated to exhibit adaptive behaviour. purposeful and individualised strategy to dealing with people. The paper describes the tools that enable ambient intelligence. This includes ambient actuation of the magnetic switches, ubiquitous computing via the device, user-centered design, and trust. This project will discuss the importance of using undetectable magnetic switches and how, by using physical principles, they can be used to protect cryptographic secrets.

II. Literature survey

[1] The electronic observing system discovers an unauthorised person entering the secured area at the dressing room entryway and emits a brief beep; the unauthorised person then needs to use a radio frequency (RF) identification card to confirm his or her identity. The RF card decoding system that is interfaced with the main CPU will recognise an authorised user when they are present and show their information on an LCD screen. A GSM module notifies the appropriate authority when an authorised user approaches a sliding door and sends information about the user, including their details. When the sliding door is opened, it immediately locks, and the user must again provide identification verification before entry is granted.

The system works by successively engaging various invisible kinds of sensors that are organised on the opposite side of the non-conducting substance through a tiny permanent magnet to activate the flashing green LED that signals that the locker is open. [2]

Solar electricity is used to power this shielding device. Solar fencing is a top choice for keeping untamed creatures out of your yard. As a consequence, protection becomes more affordable. This farm fencing is powered by solar energy, which creates electricity at such a low level that it is safe for both people and animals to be around. Anyone who enters the enclosed area and crosses the line will be shocked electrically. Additionally, it increases crop and rural area protection. The increasing security danger of today requires perimeter protection with solar fencing because it is capable of rejecting, detecting, and acting as a barrier. This technology creates and implements perimeter fencing for agricultural protection. Due to the escalating security danger, it is a modern-day necessity. It uses solar energy and has a battery reserve system so that it can continue to operate even on overcast or night time days. When a PIR or IR sensor detects an object, the controller instantly transmits a message to the appropriate individual through the GSM modem, which is interfaced with the controller. Light and alarm will both turn on simultaneously. Solar fencing can be used to regulate a generator. [3]

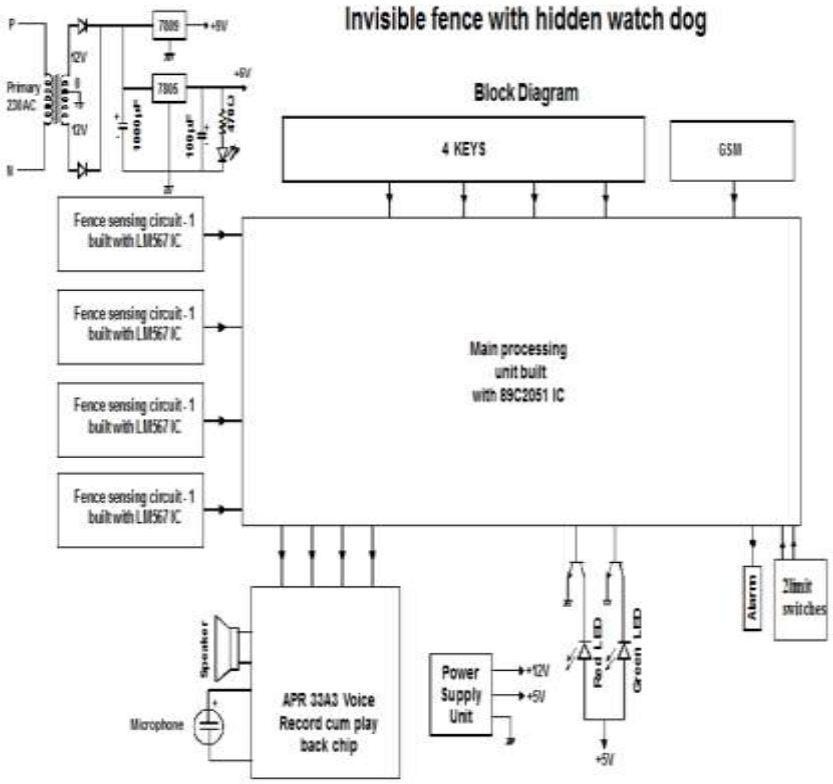
III. Methodology

The concept is to successively trigger the magnetic switches using a permanent magnet. Magnetic controls placed behind the wall are concealed from view. The switch will be activated by a magnet put near it. These toggles can be used in a variety of locations. Only those with the necessary permission are aware of where these valves are located precisely.

Each of these switches has a symbolic significance, and in order for the entrance to open, they must all be turned on. The door won't open if the incorrect code is input three times in a succession; instead, an SMS will be sent via the controller's GSM interface to the authorised mobile number specified in the controller programme.

A DC motor helps the door of the display section slide open and shut. An actual wooden plank is used to depict the wall that houses the door mechanism. A circuit board with four magnetic buttons and a microcontroller to decipher the code is located behind the board. As the magnet is moved over the board in a preset design, these switches will be activated one at a time. After the gate, a series of infrared (IR) sensors that sense the passage of a human cause the gate to close automatically.

The location of sensors is important, and they can be concealed among other items throughout the structure. Making ensuring the intruder is unaware of the devices is the aim. A audio message is played via the voice chip to acknowledge the visitor's existence when someone enters the building and walks within range of the sensors. The system instantly detects the interruption.



Block diagram

The main component of the endeavour is the five-sensor IR obstacle recognition circuit. To identify motion and automatically close the gate when someone approaches, one set is placed after the gate. Around the land, there are a total of four pairs located in various locations.

The tone encoder and tone frequency producer LM567 IC was created especially for use in the obstacle-sensing block. The obstacles are located and recorded using a variety of sensors and an IC number 567. The obstacle recognition block's IR sensors act as both infrared emitters and receivers. The walking stick has a series of these devices affixed to it. Both sensors are coupled to an IC, which generates a tone frequency of up to 20 KHz, an integrated circuit (IC) 567 that functions as a tone frequency generator and a processor is attached to both sensors. The IR signal emitter LED and the IR signal receiver LED are connected to the IC's output from the tone signal generator and the tone signal decoder, respectively, to make use of the dual capability of this IC. The component that generates the tone signal is designed as a free-running oscillator, and the directly connected resistor and capacitor values that control its frequency can be changed. A string of square vibrations starts to appear as soon as the circuit is switched on. An IR LED receives an enhanced version of this oscillator's output. The signal is released into the atmosphere by this LED, and the range can be extended by boosting the signal's intensity or emitting power. The signal from the infrared LED goes directly ahead like a laser beam, but it won't harm you.

A portion of the signal will be reflected if the laser beam's route is obstructed by an object and then picked up by the IR LED in the receiving device. The output of the receiver will instantly decrease once the output of the IC's broadcast wave is compared to the IR-output Receiver's (proportional to reflected wave). (If both are equal then output of this IC becomes low). The output of this tone encoder IC is routed to the microprocessor.

The process involves using a piece of permanent magnet to successively activate the magnetic switches. Magnetic controls placed behind the wall are concealed from view.

The switch will be activated by a magnet put near it. That kind of thing is Switch locations are adaptable. Only those with the necessary permission are aware of where these valves are located precisely. Additionally, the entrance won't open until a particular set of switches have been metaphorically turned on. If the sequence inputted is wrong three times in a row, an SMS will be sent to the authorised mobile specified in the controller programme via the GSM interfaced to the controller. Due to the GSM network's worldwide reach, users can receive communications wherever they happen to be in the world.

A DC motor helps the door of the display section slide open and shut. An actual wooden plank is used to depict the wall that houses the door mechanism. The code deciphering device, which consists of a set of five magnetic switches linked to a microcontroller, is located behind the board. As the magnet is moved around the board in a preset way, these switches will be activated one after the other in sequence. When an individual passes through an array of infrared (IR) sensors positioned after the gate, the gate automatically closes.

The microcontroller used in this project is programmed to instantly transmit a text message to the user's phone number. This is done by connecting a GSM modem to the microprocessor. The GSM module is activated by the controller when it notices the magnetic switches producing an erroneous code three times in a succession. This creates a communication connection between the mobile device and the GSM module. The controller can transmit data to multiple devices at once even though it is presently configured to send it to just one particular mobile device.

The IR emitter will continuously emit IR radiation if the sensors are close to one another, and the IR receiver will always be able to pick up the mirrored radiation as long as there is no obstacle in the way. The output will be blocked until the frequencies of the two signals converge because the IR signal cannot reach the recipient in the lack of a barrier. Therefore, the output of the 567-tone encoder will result in a logic high. The tone decoder receives the mirrored IR signal if an obstacle is put in front of the sensors, which is then caught up by the IR receiver. The output is activated, placing the internals of the IC in the ON state and grounding the circuit if the received frequency matches the produced one. A logic low signal will therefore be detected at the 567-tone encoder IC's output. Low output suggests the possibility of an invasion.

When the correct code is given, the door will open and then close once the user has entered the space. Despite the possibility of card theft with RFID readers, this approach is much more safe.

IV. Infrared Radiation

Infrared radiation has a wavelength that is longer than visible light but shorter than terahertz and microwave radiation. Red has the longest wavelength of any visible color, and since the Latin word infra means "below," the name implicitly suggests that it is below that colour. Infrared radiation has a wavelength span of roughly three orders of magnitude, from 750 nm to 1 millimetre. Humans produce radiation with a range of about 10 micrometres at room temperature.

Infrared surveillance technology is widely used in both the military and the general world. Military applications for this technology include target capture, night vision, homing, and monitoring.

Spectroscopy, remote temperature monitoring, spectral analysis, short-range radio transmission, and weather forecasting are examples of applications outside the military. Astronomers can find cold objects like planets, see through dusty regions of space like molecular clouds, and view very red-shifted objects from the early universe by using infrared instruments and sensors. The ability of infrared light to induce vibration modes in molecules by changing their dipole moments makes it useful for research on atomic-level energy levels. Using infrared spectroscopy, the absorption and propagation of light at infrared energy levels are examined.

A broad variety of infrared wavelengths are frequently released by things, but because most instruments have a tiny bandwidth, only a small part of this spectrum is useful. As a result, it is customary to further divide the infrared spectrum into focused sub-bands. The boundary between visible light and infrared radiation is not set in stone.

Since the human eye is significantly less susceptible to light with a wavelength longer than 700 nm, shorter frequencies have very little effect on landscapes illuminated by common light sources.

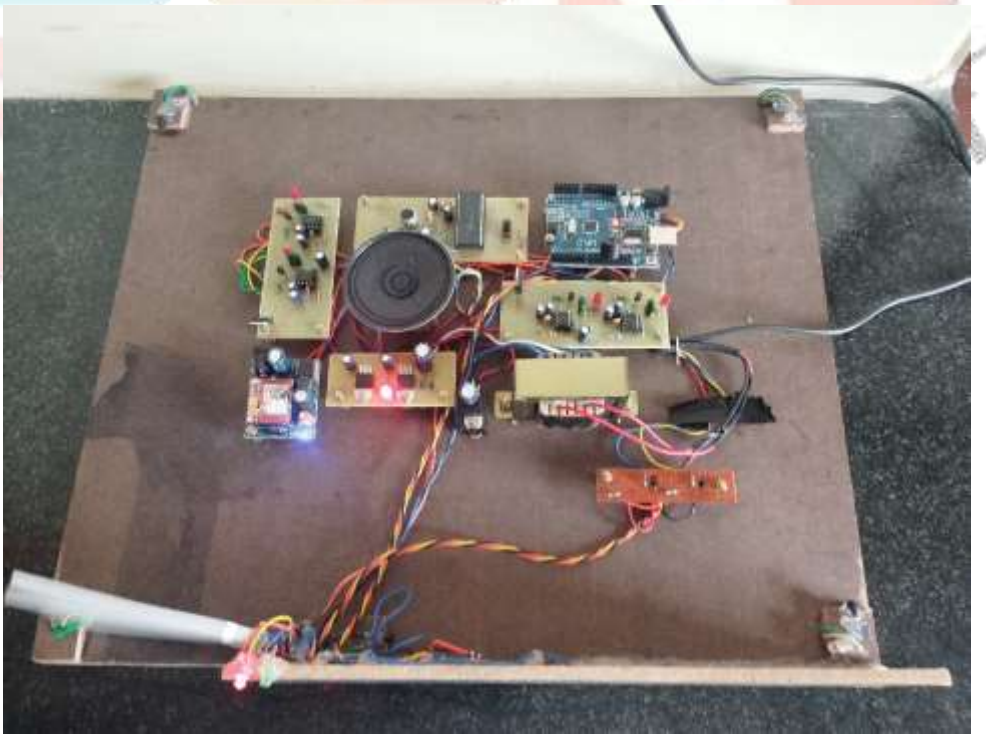
Red light, on the other hand, is visible up to about 780 nm and can be seen in very bright light. (such as from lasers or from bright sunshine with the visible light eliminated by colored gels). The infrared cutoff is estimated by a number of factors to be between 700 and 800 nm.

Because they think that all thermal heating results from infrared light and/or that all infrared radiation is a byproduct of heating, people frequently refer to infrared radiation as "heat" or "heat radiation." It's a prevalent misconception that only specific light or electromagnetic wave frequencies can cause an item to heat up. The Sun's infrared energy only accounts for 49% of the Earth's temperature increase; the remaining 71% is produced by visible light that is absorbed and then re-radiated at longer wavelengths. Lasers that generate visible or UV light can char paper, whereas incandescent objects emanate visible light. The majority of radiation from objects at room temperature will be concentrated in the 8–12 micrometre range, but this cannot be distinguished from the release of visible light by incandescent objects or UV by much higher ones.

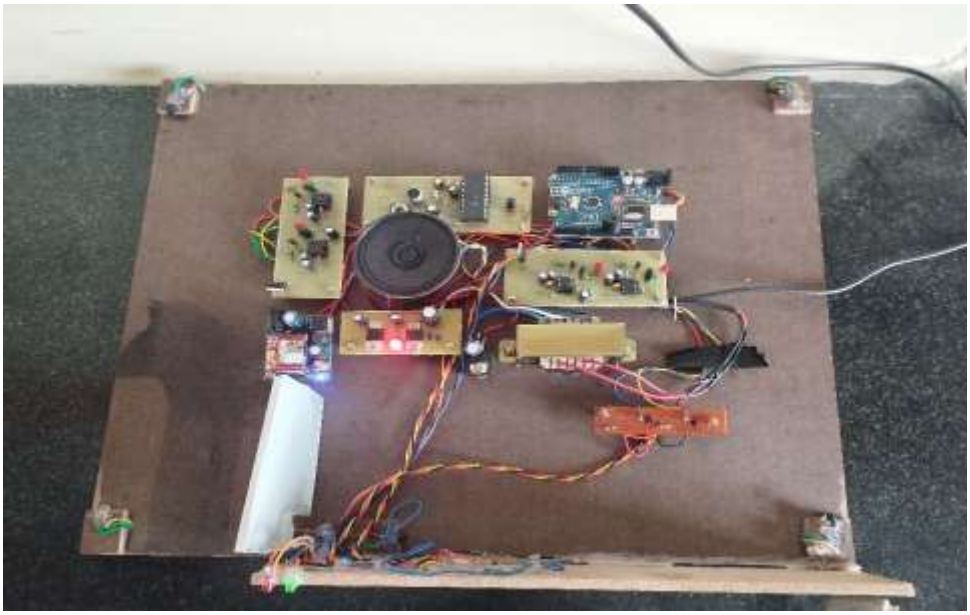
Due to their many potential applications, especially in the field of proximity sensing, infrared sensors are used in a broad range of security systems. Other important applications include numbering things and tracking rotations of rotating objects. The two primary elements of a proximity detection package are an IR LED (infrared light emitting diode) and an IR sensor (infrared light/signal receiver). (IR sensor). The device is always on because the sensor is constantly detecting light from the IR LED. A trigger circuit may be attached to the sensors to generate logic high or low pulses when something interferes with the sensors' ability to gather data. This circuit design can be applied to a range of contexts.

V. Results:

Case 1: Security on four sides using IR sensors with a gate.



Case 2: Red led at the door glows and a buzzer is given when a wrong password is provided.



Case 3: The green led at the door glows and door is opened when a correct password is given.

VI. ADVANTAGES:

- Theft is not a concern. While you are away from the office, intruders won't be able to access and take or damage anything.
- The main objective of this security system is to prevent theft of valuable business tools and sensitive data.
- If this security system is implemented, there won't be any more worry about home invasions or other unauthorised guests.

VII. APPLICATIONS:

- This technique may improve the protection of your home, apartment, and sleep.
- The highest priority in banking organisations is safety. Thus, to guarantee the highest level of safety, this method may be used.
- We can keep our most private possessions secure when we have a hidden compartment in our houses or places of work.
- Private data protection with this technology is essential.

VIII. Conclusion:

Planning and carrying out the "Invisible Fencing with Hidden Watch Dog" endeavour went off without a hitch. For display purposes, a sample module is constructed, and the outcomes are promising. A very simple section needs to be constructed because this is just a test.

Appropriate for a broad range of situations, particularly those requiring the highest level of security. We have demonstrated the importance of security in an ambient intelligent environment in this research. Security and confidence cannot be provided by cryptographic methods alone; reliable key generation and storage techniques are also necessary. The physical cloaking devices are ideal for this purpose due to their built-in security features, which include unclonability and tamper-proof evidence. Keys may be equipped with such indiscernible security measures to prevent them from being damaged by criminals or unauthorised people.

The first and most crucial task is setting up the software to perform the tasks based on the inputs. The result of the machine is entirely the responsibility of the controller's programme (code). More technological breakthroughs would be needed to create a completely working system; in this instance, technology was only used to build a prototype module.

We could include a concealed camera inside the model and then review the video to learn more about the invader. The intruder might be able to identify the magnet design, but he won't be able to locate the hidden magnets in the wall. As a result, it provides greater protection than similar devices.

REFERENCES:

1. M. W. Anwar, A. M. Khan, “Towards the Tools Selection in Model Based System Engineering for Embedded Systems - A Systematic Literature Review”, Journal of Systems and Software, vol. 106, pp.150-163, May 2015.
2. M. Rashid, M. Imran, A. R. Jafri, Turki Al-Somani, “Flexible Architectures for Cryptographic Algorithms - A Systematic Literature Review”, Journal of Circuits, Systems and Computers (JCSC), vol. 28, No. 3, March 2019.
3. Sarvesh Suhas Kapre, Saurabh Sahebrao Salunkhe, Rohan Manoj Thakkar, Akshay Prakash Pawar, Omkar Ashok Malusare, “Advanced Security Guard with PIR Sensor for Commercial and Residential use”, International Journal for Advance Research in Engineering and Technology
4. Huiping Huang, Shide Xiao, Xiangyin Meng, Ying Xiong, “A Remote Home Security System Based on Wireless Sensor Network and GSM Technology”, 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing
5. Suresh.S, J.Bhavya, S.Sakshi, K.Varun and G.Debarshi, “Home Monitoring and Security System”, ICT in Business Industry & Government (ICTBIG)
6. Freddy K Santoso, Nicholas C H Vun, “Securing IoT for Smart Home System”, 2015 IEEE International Symposium on Consumer Electronics (ISCE)
7. Invisible fencing: International Research Journal of Modernization in Engineering Technology and Science .Volume:04/Issue:06/June-2022 Impact Factor- 6.75 www.irjmets.com
8. “Security Surveillance System using Raspberry Pi and IoT Module”, Signal Processing, Informatics, Communication and Energy Systems (SPICES), 2017 IEEE International Conference.
9. Jae Hoon Lee, Yong-Shik Kim, Bong Keun Kim, Kohtaro Ohba, Hirohiko Kawata, Akihisa Ohya, Shin’ichi Yuta, “Security Door System Using Human Tracking Method with Laser Range Finders”, Proceedings of the 2007 IEEE International Conference on Mechatronics and Automation