Journal of Electrical Systems and Information Technology

RESEARCH Open Access

Design and implementation of domestic dual-SIM telesecurity alarm system using voice code recognition

Johnpaul Uzozie Okafor[1*], Akinyinka Olukunle Akande[1†] and Cosmas Kemdirim Agubor[1†]

†Akinyinka Olukunle Akande and Cosmas Kemdirim Agubor have contributed equally to this work.

*Correspondence: ifeanyijohnpaul345@gmail.com

[1] Electrical and Electronic Engineering, Federal University of Technology Owerri, Owerri, Imo State, Nigeria

Abstract

Violent crime cases which include, robbery, rape, and homicide are terribly on the rise, and the role of security in combating this menace cannot be overemphasized. This research presents a security device that aims at fighting violent crimes using voice recognition technology. The work also tends to solve the issue of network downtime when the user is out of reach for help in time of attack. In this work, a voice processing unit which comprises the condenser microphone, an amplifier, a shift register, and a timer was designed. The processing unit circuit was incorporated into microcontrollers which create Human-Device interaction and the GSM communication unit which is made up of two GSM modules. The two microcontrollers used in the design are PIC18F4520 and PIC16F873A. The microcontrollers were programmed with C++ using the MPLAB IDE software and the circuit simulation was done using Proteus Design Suite version 8. The result shows that the appropriate authority receives SMS whenever the pre-recorded code is mentioned. The result also shows that during network downtime, the second GSM module sends an SMS to the appropriate authority. Evaluating the performance of this work, it was observed that the device works best in a calm area compared to a noisy area. This work is designed to work in domestic areas like homes, offices, malls, and mainly areas free from so much noise. Therefore, this work has successfully reduced the crime rate in emergencies.

Keywords: Voice recognition, Speech recognition, Keyword spotting, Security, Communication, Violent crime

Introduction

Insecurity problem has become rampant in almost every city in Nigeria and in the world at large. There is need to proffer solutions to these deadly security threats that has eaten deep globally. Some of the security issues that are noticeable are homicide, rape, robbery and many other violent crimes [1–5]. In order to curb violent crimes, good safety practices or techniques must be applied. The rescuer should get a proper notification about the danger or intending danger and act on the information received for these practices to be effective. In many cases, people cannot tell when something wrong is happening to another person; these situations deserve proper solution. There should be proper communication between the attacked person and the people that will provide help at the material time. In a situation where nobody is there to help during the attack, a notification system becomes very important. This notification system should be able to alert people that something wrong is happening, or about to happen in a particular location.

Over the years, a lot of violent crimes have been going on especially at weird hours. Researchers have been trying to get a proper solution to these menaces [6–8]. Violent crime is an offence in which the perpetrator uses or threatens to use harmful violence against the victim [1, 9]. These violent crimes vary by country, and they include murder, sexual assault, rape, kidnapping, murder, manslaughter, robbery, and arson.

Global efforts to tackle violent crimes have intensified. This development has prompted countries around the world to implement various measures to curb violent crimes [10, 11]. These initiatives include enhancing law enforcement agencies, promoting community engagement, technological approach, and investing in education and social programs. Technological advancements have played a very crucial role in tackling crime, of all the initiatives created. Some key technological approaches are predictive policing, DNA analysis, crime mapping, gunshot detection systems, surveillance systems, biometric technology, social media monitoring, and cyber-crime prevention [10, 12, 13]. CCTV is a form of situational crime prevention [14, 36]. This CCTV will not be able to provide emergency help in critical situation because of lack of manpower to watch the screen for every home, and lack of technical know-how. Though, modern societies need police who can make good use of technology [10].

Voice recognition technology is an effective tool in fighting violent crimes at homes [15–17]. Voice recognition technology allows for the identification and verification of individuals based on their unique vocal characteristics [11, 18, 19]. Voice recognition can be integrated with artificial intelligence and natural language processing, to enhance overall crime detection capabilities. Wake word detection is a technology used in voice recognition systems to identify a specific word or phrase. This phrase serves as a trigger for activating the system [20, 21]. The aspect of voice recognition that suits this proposed telesecurity system is keyword spotting (KWS). Keyword spotting is also known as wake word detection [22–24]. Wake word detection involves continuously listening to audio input and waiting for the predefined wake word to be spoken. Once the wake word is detected, the system activates and begins processing subsequent spoken commands. Popular examples of wake words include “Hey Siri” for Apple’s Siri, “Okay Google” for Google Assistant, and “Alexa” for Amazon’s Alexa. A wake word is usually a predefined word that is fixed throughout training and detection. In KWS, the word is unknown during training and it is sometimes even when the system processes the test audio. The words can even be out of vocabulary. During the detection/test period, a wake word detection system is run in an online streaming fashion. This means that the whole word does not need to be processed before determining the presence of the wake word. The detection is started as soon as the audio stream becomes available, and report the positive trigger once a wake word is detected with high confidence, while a KWS system usually works offline and tolerates more latency. Wake word detection tasks have more restrictions in computation and memory resources than KWS due to their application scenarios [25]. These wake words are designed to be distinctive and easy for users to remember while minimizing the chances of unintentional activation. The ability to listen passively and trigger system actions are key characteristics of wake word detection.

In Nigeria, the government does not sponsor the installation of security equipment in homes. Hence, security is largely left to the discretion of the individual. The installation of physical security measures such as CCTV is clearly more difficult for poorer houses in society [26]. A remedy to the security challenges is to develop a cost-effective voice recognition security device that is user friendly, and is able to send an alert message when a wake word is detected.

This study presents the design and implementation of domestic dual-SIM telesecurity alarm system using voice code recognition. The specific objectives of study are as follows:

1. To design a voice processing unit
2. To create a human–device interaction using a microcontroller
3. To implement a GSM communication unit using dual SIM cards
4. To interconnect all the units to achieve the system
5. To evaluate the speaker dependent and speaker independent performance in both noisy and quiet areas.

This work is very important because it will help to prevent violent crimes especially in case of emergency when one is being attacked by criminals and lacks access to people outside for help. The device will simply do the task of communicating with the nearest police station, or designated phone numbers by receiving instruction (voice code) from the user. In case of network downtime in a particular service provider, the GSM communication unit switches to the second service provider for communication. It is very rare for two service providers to have network downtime at the same time.

Limitations and applicability

Applications

This device can be used in variety of locations such as in homes or offices as a wake code detector. In these locations, it can inform defined security personnel about a threatening situation on matching a pre-recorded voice code. In hospitals, it can be placed close to each patient's bed and can be triggered by some biomedical sensor. In hotels, it can be put in each room to communicate with the reception on the detection of voice code.

Limitations

The voice frequencies that trigger this work must be less than or equal to 1500 Hz. This implies that the gadget cannot be activated by the voice of a very young child.

Because there is no feature to detect motion, trespassers can effectively carry away the homeowner's personal goods when they are not present.

If there is excessive noise in the area, the device's performance will not be effective. The microphone will be unable to receive voice signals when there is noise. That's why it cannot find the essential term.

Review of related literature

Previous research has been done on home security systems, such as the development of a home security alert system by Ikpenyi [27] which uses a passive infrared (PIR) sensor to detect the presence of an intruder. The system is capable of sending an alert message to the homeowner and activating a bell alarm. This work was designed to work when the users are not home. That is to say, its main aim is property protection and not protection of the user.

Choudhury et al. [28] designed and implemented a home security system that uses SMS as a means of communication. The system is based on a microcontroller for system control and GSM technology for communication. It sends an SMS containing the emergency message and the GPS location of the sender. The project presents a versatile security and alarm system that can be used by individuals, corporations, and establishments that require a cheap but reliable security system. The project aims to provide its users with a simple, fast, and reliable way to secure their homes. This work uses just the push button approach, and this will be a barrier to communication in critical times.

Ehioghae and Ogunlere [29] designed a mobile-based home security system which was implemented using Arduino with an ATmega2560 microcontroller and interfaced with a passive infrared (PIR) sensor, a 16×2 liquid crystal display (LCD) screen, a 4×4 matrix keypad, a GSM module, and a burglar alarm to secure homes from illegal entities attempting to gain illegal entry into such homes. This work was built on per-user voice authentication, and the protection of property was the top priority of this work, not the protection of individuals. This device still will be prone to sending false alarms when the users are at home because of the motion sensor.

Falohun et al. [16] built a door security alarm system based on SMS verification and voice recognition to detect trespassers. It generates an SMS on every failed attempt to get unauthorized access to the house. This device does not have dual SIM; therefore, it is prone to not sending an SMS when there is network downtime at the time of the authorization.

Yadav et al. [30] built an Arduino-based security system for women that is activated by holding on the trigger of the device. The device is movable and portable and also tracks the current location of the user continuously. This work requires lots of money for data bundle subscription, and it also uses one GSM module which can be a serious barrier for communication in cases of network downtime.

In their research, Rashid et al. [31] built a security system that uses voice recognition as the access control key. The developed voice recognition software effectively activated the door opening mechanism using a vocal command that only works for the authenticated individual, according to the findings. The device offered medium-security access control and included an adjustable security level set to account for differences in one's speech during voice recognition. The focus of this work is on authentication of users.

Khan et al. [32] designed and implemented a low-cost home security system using GSM Network. The purpose of this invention was to provide a security device, which gives immediate notification to the owner and security services like the police station, or fire brigade at the instance of the unauthorized event occurrence detected by sensors. The protection of property was the top priority of this work and not the protection of individuals, because it was specifically designed to work in the absence of the homeowners. Also, when there is network downtime, or GSM module malfunction at the moment the incident occurred, the SMS module will not send any SMS alert to the security personnel.

Budijono et al. [33] designed a modular home security system with a short messaging system. The purpose of this design was to provide home security in the absence of the homeowners. This home security system can monitor home areas surrounded by PIR sensors and send SMS, saving images captured by a camera, and making people panic by turning on the buzzer when the area surrounded by the PIR sensor is being trespassed. The system is designed for property protection.

Ammar, Siraj, and Omar [34] developed a security mechanism intending to enhance protection, which enables owners of important premises to be notified via telephone when there is a break-in attempt, making it essentially impregnable. The possibility of network unavailability was not considered in the work.

A voice-based home security and SMS gateway using Arduino uno microcontroller and the passive infrared sensor was designed by Irawan et al [35]. The work was designed to detect trespasses in a house through a warning message (triggered by the PIR sensors) sent by the GSM module to the homeowner's cell phone so that the homeowner can find out the security status of his home. The work was recommended for effective use in a private room where valuables are found. The PIR sensor in this work will not detect any security at above 6 m distance, making it possible for criminals to trespass by forcing the homeowner to deactivate the sensor.

Table 1 displays a comparison table between this system's performance and a few of the systems that were assessed. It may be deduced from the table that the suggested system is only operational when homeowners or users are present. In other words, it is made solely with people's safety in mind, not properties. Additionally, it is noted that the inclusion of two SIM cards in the suggested system results in redundancy. In contrast to alternative designs, the suggested system is able to be activated at any given moment. System B demands that the push button be pressed without taking into account the possibility that the victim of the attack may not be around when the button is pressed.

Based on the review, the following research gaps were identified:

Table 1 Comparative table of proposed design versus related designs

System	A	B	C	D	E
AUTHOR	Okafor et al. [proposed system	Choudry et al. [28]	Yadav et al. [30]	Khan et al. [32]	Rashid et al. [31]
Dual sim (redundancy)	Yes	No	No	No	No
Reliability	Yes	Yes	Yes	Yes	Yes
Trigger	Voice command	Push button	Trigger button	PIR SENSOR	Voice command
Voice/speech identification	Authenticated keyword only	N/A	N/A	N/A	Authenticated user only
Security priority	Human	Human	Human	Property	Human & property
Internet connectivity	No	No	Yes	No	No
Internet cost	N/A	N/A	Very high	N/A	N/A
Alert mode	SMS	SMS	SMS	SMS	N/A
Emergency action	Yes	No	No	No	No

All the reviewed works integrated just one GSM module, which can become faulty at any time, or the SIM card can lose network connectivity; using dual SIM helps to remove the effect of network downtime and also mitigate the effect of SIM module malfunction.

Keyword spotting was not used as an SMS alert trigger in any of the reviewed works of literature: This work efficiently applied keyword spotting which recognizes a particular pre-recorded work and then sends an emergency message as activated by the microcontrollers.

In case of emergencies, none of the reviewed works specifically dealt with the issue of emergency attacks. But, with the help of microphones connected to strategic sections of a building, one can stay from any point and communicate with security personnel just by mentioning the wake code.

Methods

This is the specific procedure which was followed during the implementation of this work. Certain units were built dependently to be interconnected to form this system.

Design of a voice processing unit

In designing this unit, an omnidirectional sensitive microphone was used to capture voice signal. Amplification of the voice signal was done with a BC547 NPN transistor. The voice signal was converted to digital form.

For the audio input circuit design, the CZN-15E condenser microphone was used because of its high sensitivity. The value current limiting resistor of the condenser microphone (R_4) is determined using Ohms's law. The voltage is given in Eq. (1).

$$V = I \times R_4 \tag{1}$$

where $V = V_{cc} - V_o$, I is the specified current rating for the microphone (0.5 mA), $V_{cc} = 12$ V (power supply voltage), $V_o = 4.5$ V (standard operating voltage of the microphone), and R_4 is the resistance.

Substituting $V = V_{cc} - V_o$ in Eq. (1) as presented in Eq. (2)

$$Vcc - \mathrm{Vo} = I \times R_4 \tag{2}$$

Therefore,

$$R_4 = \frac{Vcc - \mathrm{Vo}}{I} \tag{3}$$

By substituting the necessary parameters in Eq. 3 as given in Eq. (4)

$$R_4 = \frac{12 - 4.5}{0.5 \times 10^{-3}} \tag{4}$$

$$R_4 = 15k\Omega \tag{5}$$

The cutoff frequency set for this design is 1500 Hz to focus on relevant signals and capture the nuances and details of the voice accurately. Experimentally proven, children from 3 to 5 years have voice frequencies ranging from 250 to 1200 Hz. Children in this age grade are old enough to operate this device while the adults have a voice frequency range of 85–255 Hz.

In order to remove DC component and allow AC which is the desired audio frequency, the capacitive reactance of the capacitor C_3 is given in Eq. (6) as:

$$X_{\mathrm{c}} = \frac{1}{2\pi F C_3} \tag{6}$$

where F is the cutoff frequency (1500 Hz), π is a mathematical constant (3.142), and C_3 is 1μF.

The value of C_3 was chosen in order to maintain the fidelity of the voice signals and reduce signal lag.

Substituting the parameters in Eq. (6) as presented in Eq. (7)

$$\mathrm{X_c} = \frac{1}{2 \times 3.142 \times 1500 \times 1 \times 10^{-6}} \tag{7}$$

$$\mathrm{X_c} = 106.08\Omega \tag{8}$$

The audio output from the transistor is guided by the transistor load line equation given in Eq. (9)

$$V_{ce} = V_{cc} - (I_c \times R_8) \tag{9}$$

Biasing at the midpoint maximizes the available collector-to-emitter voltage swing for the AC signal. This is essential for obtaining optimal gain and ensuring that the transistor operates in its linear region for a wide range of input signals.

The load resistance R_8 is presented in Eq. (10).

$$R_8 = \frac{V_{cc} - V_{ce}}{I_c} \tag{10}$$

where Vcc is 12v, $I_c = 50\mu\mathrm{A}$ (input bias current of the LM358 OPAMP), V_{ce}=6 V (amplifier output voltage, and it is normally biased at 0.5$\mathrm{V_{cc}}$).

By substituting the parameters in Eq. (11),

$$R_8 = \frac{12 - 6}{50 \times 10^{-6}} \tag{11}$$

Therefore,

$$R_8 = 120\mathrm{k}\Omega \tag{12}$$

The feedback resistor is used to set the gain of the amplification stage. The formula for the circuit gain is shown in (13).

$$A = \frac{R_f}{R_8} \tag{13}$$

where R_f=R_7 is the feedback resistance, A = 5, $R_8 = 120\mathrm{k}\Omega$

By substituting the parameters in Eq. (13), the feedback resistance is given in Eq. (14) as:

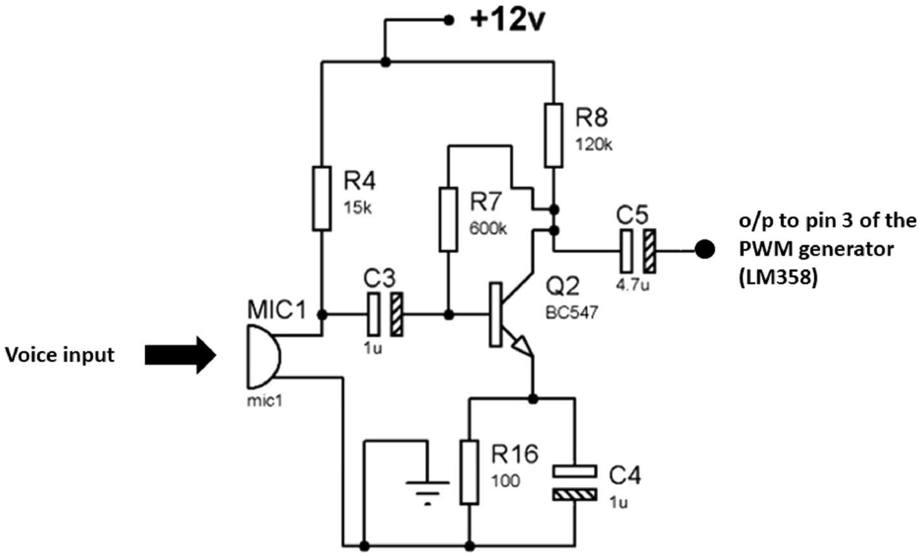


Fig. 1 Design of a voice processing and amplification unit

$$R_f = A \times R_8 \tag{14}$$

$$R_f = 5 \times 120,000\Omega \tag{15}$$

$$R_f = 600k\Omega \tag{16}$$

was chosen as the gain for proper amplification of the voice voltage from the microphone, and avoiding clipping of the amplified output voltage.

The output signal of the transistor Q2 is connected to the OP-Amp by using a coupling capacitor C5 with small capacitive reactance in order for the input impedance seen by the OP-Amp to be very small. This output goes to pin 3 of the OP-Amp as shown in Fig. 1.

The Op-Amp gets input from the coupling capacitors C5 and C8 and the ICL8038 signal generator. The input of the capacitors is the audio signal while the input of the signal generator is the triangle wave. The frequency of the triangle wave generated is equal to the cutoff frequency which is 1500 Hz.

To obtain a specific frequency for the ICL8038 signal generator, Eq. (17) is used if R1 is equal to R2 as shown in Fig. 2.

$$F = \frac{0.33}{R_1 C_1} \tag{17}$$

Therefore,

$$C_1 = \frac{0.33}{FR_1} \tag{18}$$

where F is the cutoff frequency (1500 Hz), R_1 is 6 KΩ, and 0.33 is specified in the ICL8038 datasheet.

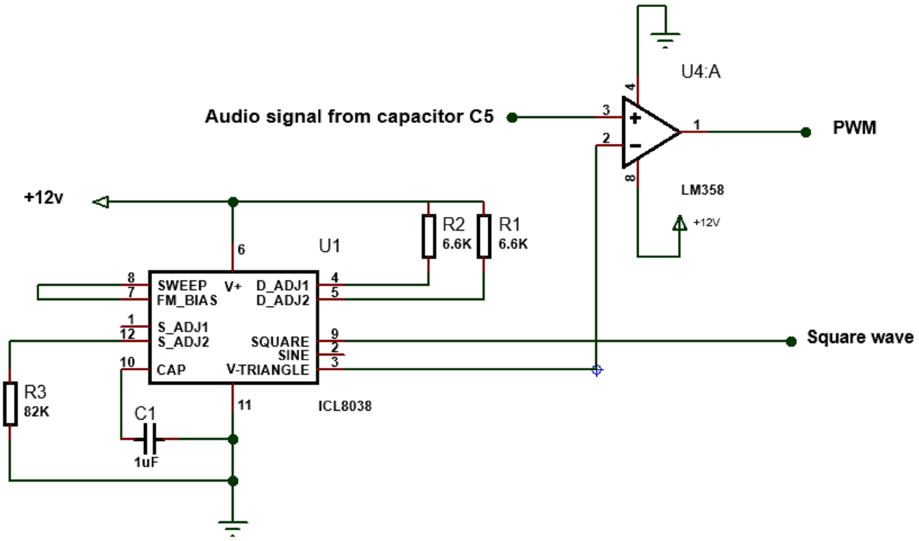


Fig. 2 Circuit diagram showing the PWM of the voice signal

$$C_1 = \frac{0.33}{1500 \times 6600} \tag{19}$$

$$C_1 = 33nF \tag{20}$$

The comparator compares the amplitude of the input signals and the result is a PWM signal whose output is either high or low.

If, triangle wave > audio signal, output = high.

If, triangle wave < audio signal, output = low.

The output will be a stream of highs and lows determined by the amplitude of the input signals.

The output signal of the PWM is referred to as vectors because it represents the voice code spoken into the microphone and presented in a digital form with unique identifier waveform. For onward processing, the vectors have to be quantized to generate a byte. The output of a 74,164 shift register depends on the state of the input and control pins and the timing of the shift and clock pulses. The PWM triangle wave signal frequency is 1500 Hz.

Therefore, the time taken for a byte of data to come in the entire 8-bit data stream of the 74,164 shift register as calculated in Eq. (21) is as follows:

$$\text{Time} = \frac{N_b}{F} \tag{21}$$

where F is the cutoff frequency (1500 Hz) and N_b is 8 which is the number of bits in the shift register.

Therefore, the time taken is presented in Eq. (22)

$$\text{Time} = \frac{8}{1500} = 5.33\text{ms} \tag{22}$$

From (22), it is observed that the higher the frequency covered, the lower the time taken for a byte of data to come in the entire 8-bit stream of the 74,164 shift register. Also, the higher the bits used for quantization, the higher the time taken for a byte to come in the entire stream of a shift register.

Creating human-to-device interaction using microcontrollers

The PIC18F4520 and PIC16F873A microcontrollers were used because they are both 8-bit microcontrollers with nanowatt technology, which means they have low power consumption and can operate in a wide voltage range (2–5.5 V). There are many microcontrollers that can be used to achieve this design, such as STM32 microcontrollers, Arduino Nano, and ATmega328P. The voice signal can be sampled using the 13-channel, 10-bit analog-to-digital (A/D) converter on the PIC18F4520 microcontroller. A synchronous serial port (SSP) on the PIC16F873A microcontroller is useful for integrating with external memory or other devices. They were both used for the design because they were both more affordable and easily accessible for purchase. The microcontroller receives the voice data in digital form from the 74,164 shift register. The firmware that are embedded in the PIC18F4520 and PIC16F873A microcontrollers written by the MPLAB IDE are executed. The implemented pin configurations for the PIC18F4520 microcontroller presented in Fig. 3 are:

i Digital voice signal from the 74,164 shift register

The microcontroller takes the voice data from the shift register. The 8 bits voice data outputs from the shift register are sent to pins 19 to 22, and 27 to 30 of the PIC18F4520 microcontroller (specified by the PIC18F4520 datasheet).

ii. Clock pulse signal from the 4022 octal counter

In order for the 4022 octal counter to capture a byte of data after 8 clock pulses and transfer to the PIC18F4520 microcontroller, its pin 10 (Q7) was connected to a digital input pin (pin 33) of the PIC18F4520 microcontroller as specified by the 4022 counter datasheet. This counter receives clock pulses at its pin 14 from the clock source (pin 8) of the shift register as specified by the data sheet of the 4022 octal counter.

iii. The keypads on the proposed device

The button keys on the body of the proposed system are configuration, voice recording, and voice search. The buttons were connected to pins 2, 34, and 35 of the PIC18F4520 microcontroller with the aid of pull-up resistors. The voltage flowing through the pull-up resistor is calculated from Ohms law as presented in Eq. (23).

$$V = I \times R \tag{23}$$

To get the pull-up resistance, R is made subject of the formula from Eq. (23). Therefore,

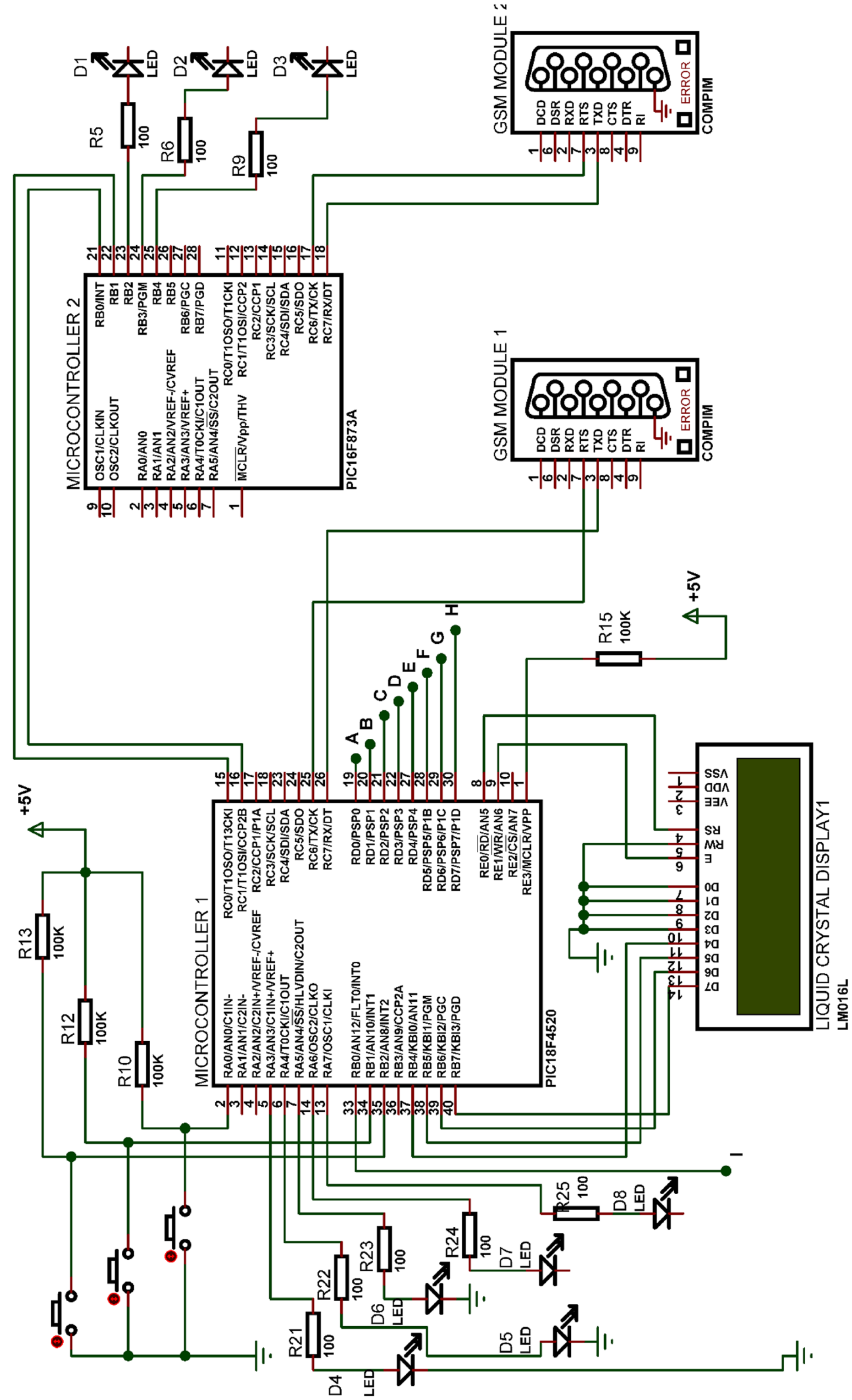


Fig. 3 Pin configuration for PIC18F4520 and PIC16F873A microcontrollers

$$R = \frac{V}{I} \tag{24}$$

where V is the output voltage from the microcontroller (5 V), I is 50 μA which is the minimum current that flows through the pull-up resistors when the pins 2, 34, and 35 of the PIC18F4520 microcontroller are grounded and $R = R10 = R11 = R12$ is the pull-up resistance.

$$R = \frac{5}{50 \times 10^{-6}} = 100\text{k}\Omega. \tag{25}$$

iv. Sending information to the (LM016L) LCD for display.

The pins 11–14 (data lines 4–7) of the LCD were connected to the pins 37–40 of the PIC18F4520 microcontroller. Pin 4 and pin 6 (register select and enable) of the LCD were connected to the pins 8 and 9 of the microcontroller as specified by the LCD datasheet.

v. The output indicators (LEDs).

The LED indicators on the PIC18F4520 microcontroller are as follows: voice record indicator, voice search indicator, voice found indicator, SIM 1 network search indicator, and SIM 1 network availability indicator. These indicators were necessary in order to see the logic output information of those pins physically. The indicators were connected to ports 5, 6, 7, 13 and 14 of the microcontroller. The choice of these pins was backed by the datasheet of the microcontroller. Different LED colors have standard operating voltages, but since different colors were used, 3.3 V was picked as the forward voltage generally.

The supply voltage V_{supply} from the microcontroller pin is 5 V. Hence, a current limiting resistor is needed to bring the voltage input to the LEDs down to 3.3 V.

The value of the current limiting resistor was determined from Eq. (23),

$$V = I \times R \tag{23}$$

where $V = V_{\text{supply}} - V_{\text{LED}}$, V_{supply}=5 V, V_{LED} is 3.3 V which if the LED forward voltage, I = 0.017A (the chosen value of 17 mA is to be on a safe side since multi-colors were used). Since all parameters are observed, R will be determined in (25) using Eq. (24).

$$R = \frac{V_{supply} - V_{LED}}{I} \tag{24}$$

$$R = \frac{5 - 3.3}{0.017} = 100\Omega \tag{25}$$

vi. The interface with the 16F873A microcontroller.

The PIC16F873A microcontroller is the second microcontroller and is connected to pin 15 and pin 16 of the main microcontroller (PIC18F4520).

vii. The interface with GSM module 1.

The GSM module 1 receiver and transmitter pins (pins 2 and 3, respectively) are connected to pins 25 and 26 (transmitter and receiver pins) to perform the operation of sending SMS.

The implemented pin configurations for the PIC16F873A microcontroller are:

i. Interface with the primary microcontroller (PIC18F4520).

In order for the dual SIM implementation to be successful, the need for sharing of work load became a necessity. The PIC16F873A microcontroller is the second microcontroller, and its pins 22 and 21 are connected to pins 15 and 16 of the main microcontroller (PIC18F4520). The baud rate was set to 9600 for proper matching.

ii. Interface with GSM module 2.

The GSM module 2 receiver and transmitter pins (pins 2 and 3, respectively) are connected to pins 17 and 18 (transmitter and receiver pins) to perform the operation of sending SMS on prompt from the main microcontroller after the SIM 1 have failed to establish network connectivity.

iii. The output indicators.

Interface with the primary microcontroller: The three output indicators connected to PIC16F873A are SIM 2 network search indicator, SIM 2 network availability indicator, and SIM 2 SMS sent. The pins are all connected in pins 23, 24, and 25 of the second microcontroller. These indicators and labels are visible on the prototype of the telesecurity system. The current limiting resistors for the three indicators are same with values derived in Eq. (25).

Implementing the GSM communication unit using dual sim cards

The GSM module 1 and module 2 were connected to the microcontrollers as seen in Fig. 3. This was to enable the modules perform the operation of sending the predefined SMS when instructed by the microcontrollers. The implemented pin configurations for the GSM modules are:

i. Sending SMS from SIM 1 and SIM 2

The transmitter port of the GSM module 1 (pin 3) was connected to the receiver pin (pin 26) of the PIC18F4520 microcontroller while the receiver pin of the GSM module 1 was connected to the transmitter pin (25) of the PIC18F4520 microcontroller as specified in the data sheets.

The transmitter port of the GSM module 2 (pin 3) was connected to the receiver pin (pin 18) of the PIC18F4520 microcontroller while the receiver pin of the GSM module 1 was connected to the transmitter pin (17) of the PIC18F4520 microcontroller.

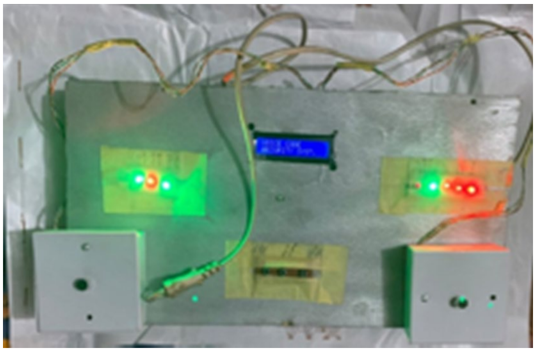


Fig. 4 Top view of the system prototype

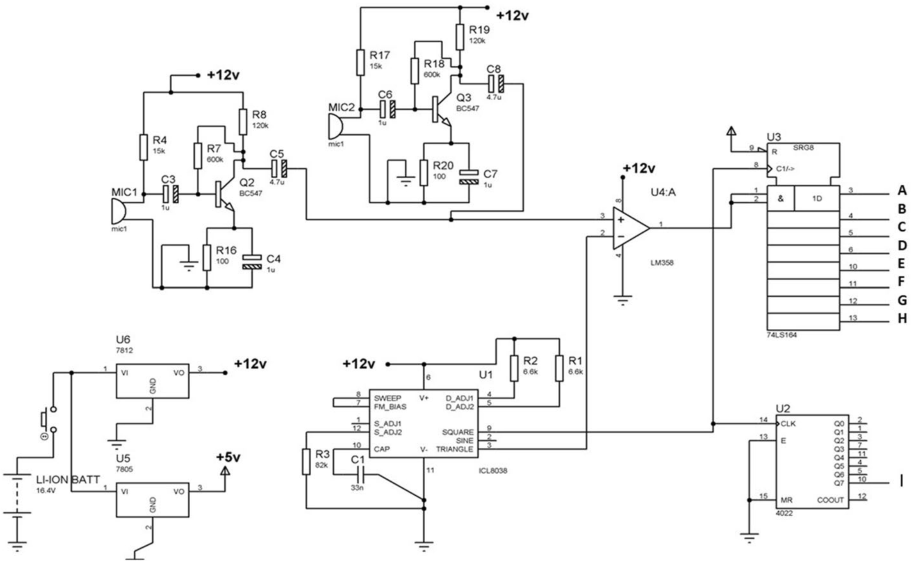


Fig. 5 Block diagram of the telesecurity alarm system

The GSM modules execute the AT commands embedded in their respective microcontrollers. The AT commands in Sect. 2.9.3 were implemented and are performed anytime the GSM module is toggled.

Interconnection of the units to form the system

The telesecurity system prototype is made up of voice processing unit, GSM modules, and microcontrollers pictorially presented in Fig. 4.

The voice processing unit converts the human voice to electrical signal and amplifies it. The amplified signal is quantized to generate digital signals. The digital signal is then transferred to the microcontroller. The microcontroller unit is the brain/processing power of the system. It equally coordinates human interaction with the system and communicates with other subsystems to achieve the project objectives. The GSM communication unit handles network activities. It is responsible for actually sending SMS to the predefined phone numbers. The power supply unit provides the necessary power supply

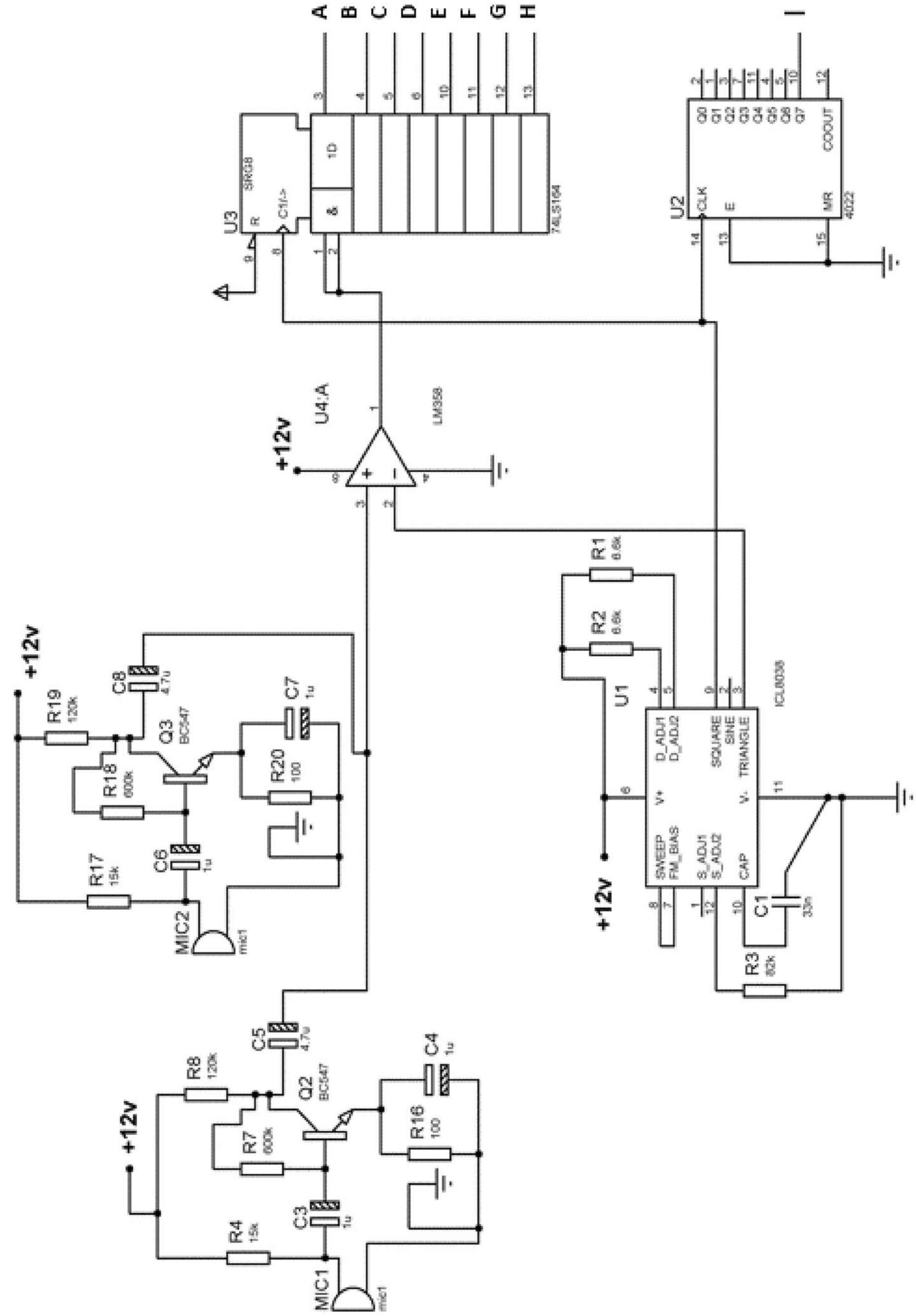


Fig. 6 Circuit diagram of the telesecurity alarm system

for the different components and units of the system. The block diagram of the telesecurity system is presented in Fig. 5.

The circuit interconnections were carried out in accordance with the specifications of the components used and the objectives of this work. The circuit diagram of this work is presented in Fig. 6. Labels A-I are the links connecting the voice processing unit and the microcontroller unit. The microcontroller unit is shown in Fig. 3. Points A, B, C, D, E, F, G, and H are the voice signals in digital form sent to the PIC18F4520 microcontroller from the 74,164 shift register. Point I is the output from the 4022 octal timer that is connected to the digital input pin of the PIC18F4520 microcontroller.

On implementation of this work, the voice signal is received, converted to electric signals, amplified, converted to digital signals, and then sent to the microcontrollers to perform its task which is to implement the firmware. After the firmware is successfully executed by the microcontrollers, an SMS result is obtained on getting a voice code match.

The flowchart of the telesecurity alarm system is a pictorial representation of the system functionalities following the same logical/sequential execution in other for the system to be effective. When the device is switched on and set for operation, it listens for the voice code. If it finds a code, it checks whether it is the programmed code. If it is not the programmed code, it keeps checking for the code. If it is the programmed code, SIM 1 is activated to send an SMS. If network is available in SIM 1, a positive result is achieved, and the process ends. If network is unavailable in SIM 1, SIM 2 is activated to send SMS alert. If network is unavailable in SIM 2, SIM 1 will be checked again. If network is available in SIM 2, SMS alert will be sent, and a positive result is achieved, and the process ends. All these explanations are diagrammatically explained in Fig. 7.

Evaluation of device performance

A speaker-dependent test and speaker-independent test were carried out on the telesecurity alarm system prototype. Speaker-dependent test determines whether it detects the voice of only one user. While speaker-independent test determines whether it detects the voices of multiple users. This was performed both in noisy and calm areas for the speaker-dependent and the speaker-independent test.

Results and discussion

SMS result

Once a voice code is found, the microcontroller asks the GSM module to check for network availability using the AT command syntax. An SMS is sent to the predefined phone numbers thereafter if network is available. The microcontroller asks the second GSM module to send the SMS if the GSM module does not find a network. The preprogrammed phone numbers then receive the SMS as shown in Fig. 8.

Evaluation of performance

The result of the speaker-independent test in both calm and noisy areas is shown in Tables 2 and 3, respectively. One of the users pre-recorded the voice code, and another user's speech was used to match the code. The users' voices were tagged "User A" and "User B," respectively, as shown in Tables 2, 3, 4, 5.

i. Speaker-independent test

This test was carried out to check the code recognition accuracy of the domestic dual-SIM telesecurity alarm system (DSTAS) from different users. This test is necessary to enable multiple users to be able to use the device. In a standard house, there should

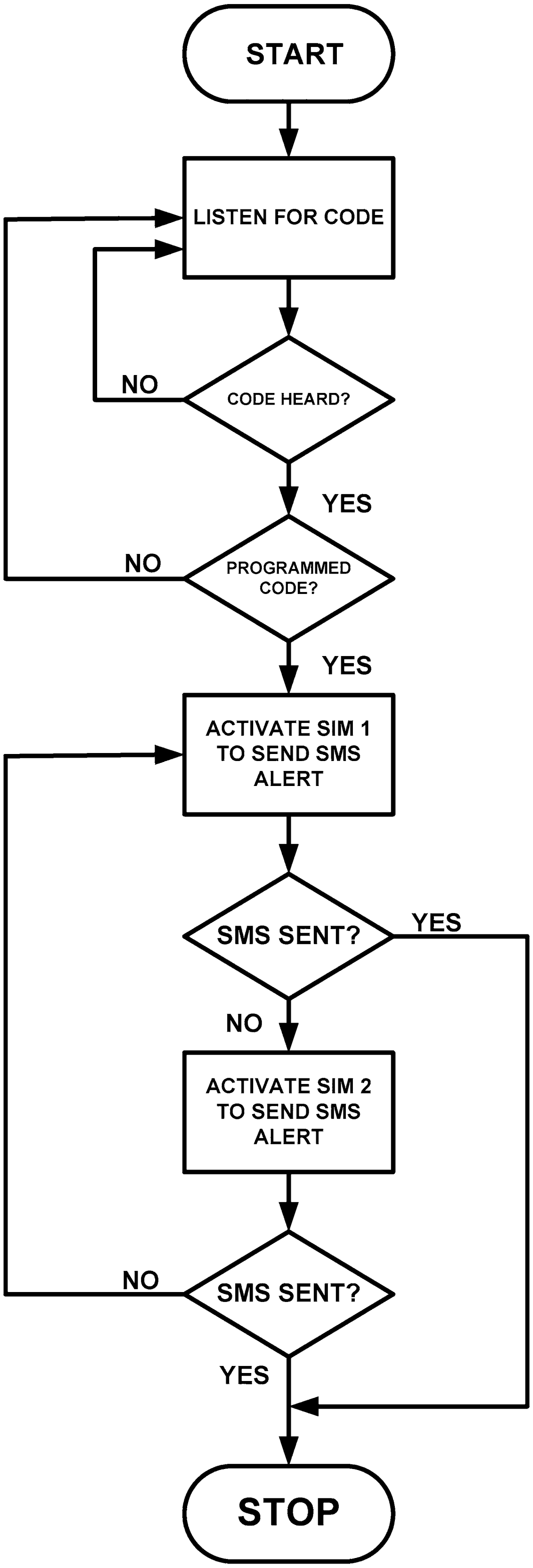
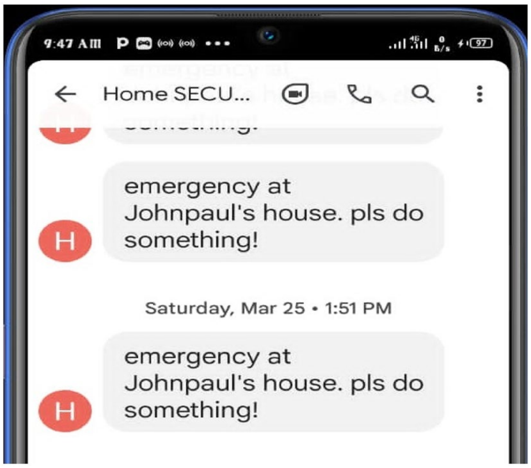


Fig. 7 Flowchart of the telesecurity alarm system



emergency at Johnpaul's house. pls do something!

Saturday, Mar 25 • 1:51 PM

emergency at Johnpaul's house. pls do something!

Fig. 8 SMS result sent to a predefined phone number

Table 2 Speaker-independent test in a calm area

TRIAL	1	2	3	4	5	6	7	8	9	10
USER A (Pre-recorded code)	Bat	She	Gib	Mow	Ket	Pee	Tom	Ash	Gib	Tom
USER B (Match result)	Pass	Fail	Fail	Pass	Pass	Pass	Fail	Pass	Pass	Pass

Table 3 Speaker-independent test in a noisy area

TRIAL	1	2	3	4	5	6	7	8	9	10
USER A (Pre-recorded code)	Bat	She	Gib	Mow	Ket	Pee	Tom	Ash	Gib	Tom
USER B (Match result)	Fail	Fail	Pass	Fail	Pass	Pass	Fail	Fail	Fail	Pass

Table 4 Speaker-dependent test in a calm area

TRIAL	1	2	3	4	5	6	7	8	9	10
USER A (pre-recorded code)	Why	Pee	Zug	Mow	Gib	Pat	Tom	Ash	Ton	Tom
USER B (match result)	Pass	Pass	Fail	Pass	Pass	Pass	Fail	Pass	Pass	Pass

Table 5 Speaker-dependent test in a noisy area

TRIAL	1	2	3	4	5	6	7	8	9	10
USER A (Pre-recorded code)	Why	Pee	Pee	Mow	Gib	Pat	Tom	Ash	Ton	Tom
USER B (Match result)	Fail	Fail	Pass	Fail	Pass	Pass	Fail	Pass	Fail	Pass

be more than one person at home. So, the test was carried out to see how accurate the DSTAS device will perform when different users operate it with the known voice code. Table 2 shows that there are 7 passes out of 10 trials compared to the 4 passes out of 10 trials in Table 3. These results depict that the presence of noise reduces the efficiency of the device. It also depicts that the device captures the speech of the users and not the voice of a particular user.

ii. Speaker-dependent test

This test was carried out to know the system functionality. It was necessary because the DSTAS needs to be functional first for a user before diversifying. These test results are shown in Tables 4 and 5. Table 4 shows 80% accuracy, while Table 5 shows 50% accuracy. This is a result of background noise. Noise can vary from mild to loud, to extra loud—making the positivity of the result unstable.

Generally, as observed from results in Tables 2, 3, 4, 5, the device might not decode a word due to voice frequency variation. In Table 2, the result of the third trial changed from negative to positive, meaning that something made the device not decode the same word initially which might be a result of low battery, or device malfunction, or that the code pattern was inappropriately pronounced. It is important to note that no voice recognition system can be 100% efficient.

Conclusions

The design and implementation of a dual-SIM telesecurity alarm system using voice code recognition have made a breakthrough in the world of security and voice recognition when it comes to its ability to help victims in emergencies: its lower cost of implementation and maintenance, its capacity to be able to withstand the effect of network downtime, and its ability to be speaker-independent when voice matching is a big gain. After testing the work, results showed that noise and voice frequency variations are big limitations that affect the result of the device negatively. The result of this work is simply to send an SMS alert to the predefined phone numbers. This device is always active, waiting for a trigger (voice code) so that it will activate the SMS.

Abbreviations

DSTAS	Dual-SIM telesecurity alarm system
KWS	Key-word spotting
SMS	Short messaging service
PIR	Passive infrared sensor
USB	Universal serial bus
SRAM	Static random-access memory
EEPROM	Electrically erasable programmable random-access memory

Acknowledgements
Not applicable.

Author Contributions

C.K., J.U., and A.O. collectively named the work. C.K. and J.U. worked on the abstract. J.U worked on the introduction, methods, results and discussion, conclusion, and compilation of the entire work. C.K., J.U., and A.O. worked on the reviewed literature. C.K. and A.O. vetted the work.

Funding
Not available.

Availability of data and materials
Not applicable. This is a design work. So, no data were collected. All results obtained after testing the device are recorded under the "Results and Discussion" section.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
On behalf of all authors, the corresponding author declares that there is no conflict of interest.

Received: 27 October 2023 Accepted: 20 February 2024
Published online: 05 March 2024

References
1. R Rosenfeld 2009 Violent crime Oxford Bibliographies Online Datasets https://doi.org/10.1093/obo/9780195396607-0001
2. J Roach K Pease 2011 Evolution and the prevention of violent crime Psychology (Irvine, Calif) 02 04 393 404 https://doi.org/10.4236/psych.2011.24062
3. MA Oyinloye SA-A Adegboyega FO Akinluyi AA Komolafe JO Akinyede OO Aladejana AO Akande 2023 Detection and mapping of violent crime hotspots in southwestern Nigeria J Geogr Inf Syst 15 03 334 365 https://doi.org/10.4236/jgis.2023.153017
4. B Knight A Tribin 2023 Immigration and violent crime: evidence from the Colombia-Venezuela Border J Dev Econ 162 103039https://doi.org/10.1016/j.jdeveco.2022.103039
5. CO Ugwuoke BO Ajah L Akor SO Ameh CA Lanshima EC Ngwu UA Eze M Nwokedi 2023 Violent crimes and insecurity on Nigerian highways: a tale of travelers' trauma, nightmares and state slumber Heliyon 9 10 e20489 https://doi.org/10.1016/j.heliyon.2023.e20489
6. R Roth DL Eckberg CH Dayton K Wheeler J Watkinson R Haberman JM Denham 2008 The historical violence database: a collaborative research project on the history of violent crime, violent death, and collective violence Hist Meth 41 2 81 98 https://doi.org/10.3200/hmts.41.2.81-98
7. JC Wood 2017 Future agendas for research on violent crime: the challenge to history from evolutionary psychology Crime, Hist Soc Crime Hist Soc 21 2 351 359 https://doi.org/10.4000/chs.2036
8. JD Rosen HS Kassab 2019 History of crime and violence Drugs Gangs Viol https://doi.org/10.1007/978-3-319-94451-7_2
9. PM Shanti S Balaselvakumar K Kumaraswamy 2021 A study on violent crimes in Tiruchirappalli city, Tamil Nadu Sci Technol Dev 10 02 393 424
10. AO Akande CK Agubor WA Ahmed O Ogunbiyi 2023 Performance of cooperative relay protocol in 5G mobile communication network over Rayleigh fading channel Int J Mob Commun https://doi.org/10.1504/IJMC.2023.10042868
11. MA Umar A Aliyu Machina M Ibrahim JA Nasir A Saheed Salahudeen M Mustapha I Shuaibu 2021 Fighting crime and insecurity in Nigeria: an intelligent approach Int Comput Eng Res Trend https://doi.org/10.5281/ZENODO.4665972
12. CK Agubor AO Akande CR Opara 2022 On-off switching and sleep-mode energy management techniques in 5G mobile wireless communications—a review IJ Wirel Microw Technol 6 40 47 https://doi.org/10.5815/ijwmt.2022.06.05
13. Anderez DO, Kanjo E, Amnwar A, Johnson S, Lucy D (2021) The rise of technology in crime prevention: opportunities, challenges and practitioners perspectives. https://doi.org/10.48550/ARXIV.2102.04204
14. R Vijeikis V Raudonis G Dervinis 2022 Efficient violence detection in surveillance Sensors (Basel, Switzerland) 22 6 2216 https://doi.org/10.3390/s22062216
15. F Jansen J Sánchez-Monedero L Dencik 2021 Biometric identity systems in law enforcement and the politics of (voice) recognition: the case of SiiP Big Data Soc 8 2 205395172110636 https://doi.org/10.1177/20539517211063604
16. A Falohun B Makinde T Akin-Olayemi F Akinleye TM Oyelami 2020 Design and implementation of a mobile-based home security system Int J Adv Res Comput Sci Am Sci Res J Eng Technol Sci 72 3 101 112
17. T Santosh G VedhaSree A Bhargavi AGS LikithaSivani T Santosh 2023 Design and implementation of voice recognition based security system Ind Eng J 52 5 1404 1415
18. CK Agubor AO Akande R Opara 2021 Interference mitigation in wireless communication–a tutorial on spread spectrum technology Inter J Wirel Microw Technol 5 26 34 https://doi.org/10.5815/ijwmt.2021.05.04
19. MM Kabir MF Mridha J Shin I Jahan AQ Ohi 2021 A survey of speaker recognition: fundamental theories, recognition methods and opportunities IEEE Access Pract Innov Open Sol 9 79236 79263 https://doi.org/10.1109/access.2021.3084299
20. AO Akande OK Akinde OO Joel IA Okiki-ade AM Olusegun AS Adeola 2023 Development of a modified propagation model of a wireless mobile communication system in a 4G network Int J Electr Comput Eng 13 6 6489 6500 https://doi.org/10.11591/ijece.v13i6.pp6489-6500

21. Hossain D, Sato Y (2021) Efficient corpus design for wake-word detection. 2021 IEEE Spoken Language Technology Workshop (SLT). Presented at the 2021 IEEE Spoken Language Technology Workshop (SLT), Shenzhen, China. doi:https://doi.org/10.1109/slt48900.2021.9383569
22. I López-Espejo Z-H Tan J Hansen J Jensen 2021 Deep spoken keyword spotting: an overview https://doi.org/10.48550/ARXIV.2111.10592
23. T-H Tsai P-C Hao C-L Wang 2021 Self-defined text-dependent wake-up-words speaker recognition system IEEE Access Pract Innov Open Sol 9 138668 138676 https://doi.org/10.1109/access.2021.3117602
24. Y Li J Ren Y Wang G Wang X Li H Liu 2023 Audio–visual keyword transformer for unconstrained sentence-level keyword spotting CAAI Trans Intell Technol https://doi.org/10.1049/cit2.12212
25. Akinde OK, Okafor KC, Akande AO (2019) Automated bomb detection system for composite terrorist disarmament (CTD). Int J Mechatro Electr Comput Technol 9(34)
26. A Tseloni R Thompson L Grove N Tilley G Farrell 2017 The effectiveness of burglary security devices Secur J 30 2 646 664 https://doi.org/10.1057/sj.2014.30
27. OE Ikpenyi OE Abumere JA Amusan 2022 Construction of GSM based home security alert system using passive infrared sensor World J Adv Res Rev 14 2 648 657 https://doi.org/10.30574/wjarr.2022.14.2.0447
28. Choudhury B, Choudhury TS, Pramanik A, Arif W, Mehedi J (2015) Design and implementation of an SMS based home security system. 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT). Presented at the 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India. https://doi.org/10.1109/icecct.2015.7226115
29. E Ehioghae S Ogunlere 2021 Design and construction of a door security alarm system based on SMS verification and voice recognition Int J Adv Res Comput Sci 12 3 23 37 https://doi.org/10.26483/ijarcs.v12i3.6705
30. DM Yadav G Neha D Sujay 2022 Security system with voice recognition and autodialing Math Stat Eng Appl 71 4 13191 13197
31. Rashid RA, Mahalin NH, Sarijari MA, Abdul Aziz AA (2008) Security system using biometric technology: design and implementation of Voice Recognition System (VRS). 2008 International Conference on Computer and Communication Engineering. Presented at the 2008 International Conference on Computer and Communication Engineering (ICCCE), Kuala Lumpur, Malaysia. https://doi.org/10.1109/iccce.2008.4580735
32. SR Khan A Al Mansur A Kabir S Jaman N Chowdhury 2012 Design and implementation of low cost home security system using GSM network Int J Sci Eng Res 3 3 1 6
33. S Budijono J Andrianto MA Noor 2014 Design and implementation of modular home security system with short messaging system EPJ Web Conf 68 00025 https://doi.org/10.1051/epjconf/20146800025
34. M Ammar M Siraj SM Omar 2012 Design and implementation of modern security system based on mobile phone J Eng Sustain Develop 16 4 314 329
35. Y Irawan Y Yulisman N Belarbi MM Josephine 2021 Voice-based home security and SMS gateway using arduino Uno microcontroller and passive infra red sensor J Appl Eng Technol Sci (JAETS) 3 1 19 25 https://doi.org/10.37385/jaets.v3i1.269
36. M Khairy RM Al-Makhlasawy 2022 A reliable image compression algorithm based on block luminance adopting deep learning for video surveillance application J Electr Syst Inf Technol https://doi.org/10.1186/s43067-022-00063-0

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.