Journal of Computer Science

Review

Review on Home Security System in Developing Countries: Affordability or Comfortability

[1,5]Moses Eterigho Emetere, [2]Daniel Chidera Okpala, [3]Muhammad Muhammad Bakeko and [4,5]Sunday Adeniran Afolalu

[1]Department of Physics, Bowen University, Iwo, Osun State, Nigeria
[2]Department of Physics, Covenant University, Ota, Ogun State, Nigeria
[3]Department of Physics, Federal Polytechnic, Bida, Niger State, Nigeria
[4]Department of Mechanical Engineering, Afe Babalola University, Ado-Ekiti, Ekiti State, Nigeria
[5]Department of Mechanical Engineering Science, University of Johannesburg, APK Campus, Johannesburg, South Africa

Article history
Received: 18-12-2021
Revised: 22-02-2022
Accepted: 31-03-2022

Corresponding Author:
Moses Eterigho Emetere
Department of Physics, Bowen University, Iwo, Osun State, Nigeria
Email: emetere@yahoo.com

Abstract: The spate of robbery, kidnapping, and killing has increased tremendously as most developing countries live below the poverty index. Relying on local authorities may be suicidal as global security architectures have noticeable imperfections. Hence, when planning security solutions on an individual or community basis, the cost is the main factor that must be considered. This review seeks to proffer solutions adapted to little communities to abate or mitigate crimes. The need for an unmonitored home security system was discussed as it has been identified as the panacea to curb organized crimes. Available security technologies were discussed in chronological order, focusing on affordability or comfortability. In developing countries, low-income earners are the victims; the security option should be centered on affordability. On the other hand, average-income earners who could afford the cost of newer technology are plagued with social burdens and time consumption in scanning and updating the biometrics of their guests. In that case, the challenge becomes 'comfortability'. This review examined the shortcoming of home security systems and how it applies to curbing crimes. Low-cost home security was then proposed with all its components, languages, and tools listed for further work. It is recommended that incorporating a shared database with old technologies' home security systems would lead to 'affordability' and 'comfortability'. This recommendation can reduce crimes by 30%.

Keywords: Home Security, Affordability, Comfortability, Technology

Introduction

Today, the world faces insecurity, with the ever-increasing rate of crime as a problem (Ruth, 2021). Third-world countries are in no way excluded from this problem. The failing economy and high unemployment rate in the country have left country with unprecedented growth in crime rates of every kind. Inadequate efforts are being made to proffer a solution to this problem. This shortcoming, i.e., insufficient technology utilization, has made the security sector a failure. Most third-world countries struggle with other problems such as poverty, underdevelopment, lack of utilization of advanced forms of technology (artificial intelligence to be precise), and the failure of the government to integrate technology with the country's security sector.

All the above-stated problems are related to the problem of insecurity in the sense that currently, the security agencies in most developing countries still have stale approaches to forensic investigations, being unable to gather quality data from crime scenes and analyze this data through science and technology-aided methods. So even after a crime has been committed, the possibility of narrowing down to a suspect with just biometric features found at the crime scene is very low and impossible in most cases. Most of the investigations carried out require witnesses to be present at the crime scene or the victim to identify with a suspect to guarantee its success. In cases where there are no witnesses and the victim was absent when the crime was being committed (cases of burglary), the criminal has a high chance of getting away while sourcing for the next victim. Hence, the need to identify these criminals somehow (Peterson *et al*., 2010).

The two major types of home security systems exist monitored and unmonitored security systems. Monitored

security systems are systems that a professional home security company actively monitors. Unmonitored (or self-monitored) security systems consist of equipment you can have a professional install or install yourself. The primary advantage of unmonitored security systems is the cost mainly of the company's monitoring service. Equipment requirements for the unmonitored security system can vary significantly between systems, but typical items include a control panel, motion sensors, door and window sensors, glass-break sensors, smoke detectors, and sirens. The latest systems use the latest wireless communication like bluetooth, infrared, and Wi-Fi access. Hence, with a smartphone-compatible device i.e., events can be monitored from the system remotely (Zhao and Ye, 2008; Bangali and Shaligram, 2013). This can be the system's primary disadvantage, especially when the person is indisposed due to phone coverage area, etc. The second disadvantage is that even though it might alarm the owner of unusual activity and ward off trespassers, it will not prevent a crime from taking place or even prevent further damage. The advantage of a monitored system is the convenience of allowing hired company-run protocols even at odd hours. For third-world countries, the cost is a major factor in choosing a home security device. Based on the above research, unmonitored security is improved upon in several ways to meet users' convenience (Al-Ali *et al*., 2004; Doknić, 2014).

In the case of poverty, with almost half the country struggling to survive, ordinary people fail to see the need to invest any form of finance in security, and those who barely spare money do not invest in very efficient forms of security. The common security most homes offer in this current day is locked doors, which can still be broken into at any time with the burglar running free afterward and unidentified. Any more advanced form of security that utilizes any form of technology is expensive and only financially buoyant people can afford these. Moreover, even when implemented in homes is still complex to operate, which would result in extra expenditure to maintain it and hire technically skilled experts. This idea undoubtedly makes it almost impossible for average-class citizens to afford any form of technology-aided security for their homes.

As of today, most developing nations of the world are yet to invest richly in the rapidly growing field of artificial intelligence (Lee and Cho, 2017). There are hardly any homes that invest in automated systems or the internet of things. Such systems are expensive and complex to operate. This complexity more often is due to the high level of technological illiteracy in the country, making it hard for an average person to comprehend and operate such systems, and here is where the high cost of maintenance kicks in. For this reason, it is easy to overlook the benefits of implementing technology-aided security. Furthermore, some people live in sylvan areas, where there are fewer people. In areas like these, a break-in can be easily made unnoticed. Also, an escape can be made easily, owing to the unavailability of people in those areas. Different kinds of crimes can be easily committed in such areas because, more often than not, there are no witnesses and the chances of identifying these people afterward are low.

This review seeks to solve these problems by utilizing biometrics technology, as biometrics technology proffers the best solution to the problem. With this, homeowners can have better solutions to their security problems and have more control over their homes. With successful biometrics identification, homeowners can get quick notifications of imminent threats to them or their homes and at this point, seek ways to evade danger. It does not matter the person's location, as this review suggests IoT (internet of things) as an effective tool to actualize a formidable security architecture (Fornasier, 2020). A homeowner can actively keep watch of his or her home from anywhere in the world. Moreover, even after perpetrating a crime, culprits can still be identified and duly punished afterward. Also, implementing such a system is bound to offer more benefits than just identifying threats. A house owner (parent) can keep a better watch on the family members, especially the underage kids, and monitor the access of visitors and friends. The Proposed Home Security System (PHSS) uses face recognition to identify (as a threat or not) people accessing a house while notifying the homeowner of such presence. Necessary action can be taken as regards who was identified. The PHSS uses a raspberry Pi board as the microprocessor, a PIR motion sensor to detect the presence of people near a door or window, and a camera module to capture image frames of the area until there is no more motion. The capture frames are then processed, then faces in the image are detected, extracted, stored, and checked for recognition. During this time, a notification is sent to the house owner or occupants, notifying them of the person's identity being recognized. During cases where such a person is unable to be identified, the user would be prompted to identify such a person if known to him or her. Data collected at the point would be utilized when next the person is recognized by the system. An alternative way would be to stream the camera capture as a video and detect all faces present.

Images taken by the camera will be sent through an HTTP post request to a C # application, which will attempt to recognize the face extracted from the images and store the images in a SQL server database. Using Emgu CV and accord.Net libraries, faces from the images will be detected, extracted, and then identified for this PHSS. Notifications can then be sent to occupants with processed results through their emails. The scope of the review is to provide better security options that can easily be made available to homes in developing countries. Programming skills will be required in the overall design

and this PHSS as there will be back-end code for processing images and communicating with the database. It will use a raspberry Pi board interfaced with a database and web browser, a PIR sensor for detecting the human presence, a camera module for taking snapshots of the required area, and established communication with the face recognition application and database.

State of Crimes in Third World Countries

There has been an alarming growth of crimes in third-world countries. Crimes in third-world countries have a subtle influence on increased crimes in neighboring countries. For example, between 2011 and 2012, the crime rate in Nigeria rose from 65.93 to 66.28% and reached 66.45% in 2013 (Metu *et al*., 2018). This growth over the years calls for the need to adopt more efficient means of curbing crimes in Nigeria as traditional means are not efficient. The same scenario has been replicated in most parts of the world as the most common crimes include robbery, assault, burglary, murder, armed robbery, bribery and corruption, manslaughter, felonious wounding, kidnapping, etc. Figure 1 shows the crime statistics between the years 2007 and 2015 in Nigeria.

Technology is currently playing a major in the prevention and tracking of crime and the apprehension of criminals. With the growth of technology, new methods, and tools are discovered that aid justice and law enforcement worldwide.

Technology has provided surveillance, monitoring, and detection systems, which can either curb crime or solve criminal cases:

- Closed-Circuit Television (CCTV) cameras for surveillance have proven very useful during the past years. Areas that require surveillance can be monitored to either stop people from committing crimes or aid investigations if a crime is still committed. This idea would require that camera be strategically placed. A criminal investigation would consist of a set of questions: Who was responsible or involved in the crime, what transpired, when did the crime occur, why did the crime happen, and where the crime happened; this is known as the five-Ws investigation model. CCTV comes in handy to answer two of the questions, namely questions involving who and what (Ashby, 2017). CCTV cameras are also used to monitor the behavior of inmates and potentially dangerous patients in medical facilities
- Drones are being adopted for operations in a lot of sectors, including security. There are many ways drones can be used to elevate security. Drones are being used in dangerous missions since the lives of people who would have otherwise been put in harm's way using manned vehicles are protected. (Rani *et al*., 2016) as alternatives to helicopters to get aerial views of scenes. Other ways in which drones are used are risk assessment, perimeter control, maritime surveillance, traffic surveillance and management, event security, anti-poaching operations, remote area inspection
- Gunshot detection technology is also being used to advance security and curb crime. It is designed to detect and notify law enforcement authorities of the details of the discharge of a firearm. This idea includes the location and the time of the occurrence that is achieved by an interconnected system of acoustic sensors placed on elevated erections. However, this is done with the consent of the property owners (La Vigne *et al*., 2019)
- Global positioning systems are used to track criminals and locate crime scenes quickly
- License plate scanning enables the police or law enforcement agents to monitor vehicles more efficiently. A stolen vehicle can easily be discovered through license plate scanning, or a wanted driver could easily be apprehended
- Also, through machine learning and big data, crime patterns and trends can be analyzed and predicted and appropriate actions are taken
- Through machine learning, biometrics technology, and biometrics data such as faces, fingerprints, DNA, etc., people can now be recognized by machines, making it easier to track and identify criminals

Shortcomings and Prospects of Home Security Systems

Automated home security systems are being adopted in many homes worldwide as they are a better security option than conventionally locked doors and fences. Many of these systems in use today can be operated wirelessly and can be easily installed.

As artificial intelligence is finding its way into every field of human endeavor, home security is not left out. Some home security systems use some form of artificial intelligence to operate smartly. As home security systems are further improved, robbery and burglary crimes in homes would be harder to perpetuate and easier to follow up on. Home security systems provide all-around 24/7 security, which is impossible with employed guards. These systems can provide surveillance and monitoring, even when homeowners are away. One extra advantage of these systems is that they protect against burglars and come with sensors that can detect smoke, flood, gas, or fire and set off alarms or notify homeowners through GSM. While power outages could be a problem, wireless security systems run on batteries, especially in developing countries. That is to say, homes can still be protected and monitored during power outages. Houses with security systems are also less likely to be burgled. High decibel alarms can scare intruders off in such cases where there is still a break-in attempt. Most security systems provided by companies are linked to the monitoring center for which law enforcement agents are notified of a suspected break-in.

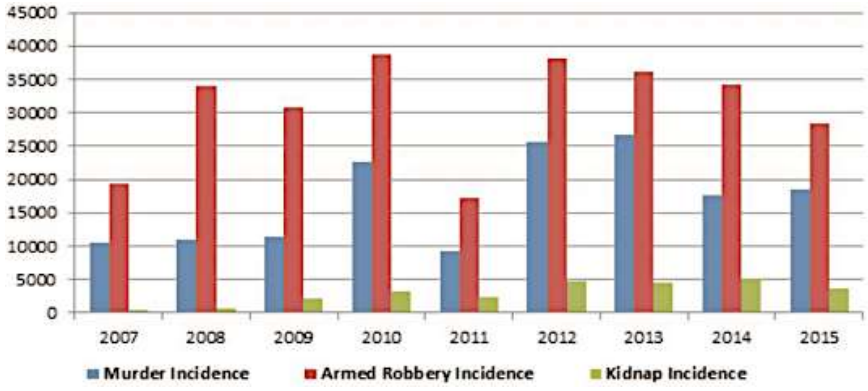

Fig. 1: Incidents of crime in Nigeria (2007-2015) (WDI, 2016)

However, these systems can be quite expensive to install and maintain. That is to say that the rate charged by companies providing these services is often high and affordable for everyone. Users usually have to subscribe to a monthly or yearly payment plan in addition to the cost of installation and maintenance. Although DIY systems are much cheaper, the cost of batteries for wireless systems should still be taken into consideration. Also, these systems are subject to false alarms. That is to say that alarm systems give off false alarms when even a family member enters the restricted area. Moreover, these systems can also fail at detecting the presence of a visitor or stranger. These could make homeowners less wary in case of an actual threat. Burglars are becoming skilled at cutting wires can to disable security systems and noting common locations for motion sensors and either disabling or avoiding them. Wireless systems are susceptible to signal interference and hacking. Some systems are unmonitored and are not very efficient in places where alarms set off cannot be reported in case of the homeowner's absence. Wired systems, unlike wireless systems, do not rely on batteries and so cannot provide surveillance in times of power outage.

Role of Artificial Intelligence in Home Security

The integration of artificial intelligence with home security systems has enabled smarter security systems capable of performing certain security tasks without constant supervision. The shortcomings mentioned above of home security systems, such as false alarms and detections, can be improved with artificial intelligence. Generally, security systems can be improved with the use of artificial intelligence. Break-ins can be detected using sensors and facial recognition technology identifies the person (s). Not only this, objects and people caught on camera can also be identified through machine learning while homeowners are identified. This idea helps homeowners keep better track of activities around their homes and eliminates the need to sit and watch security footage for hours. With the aid of voice assistance, homeowners can better interact with their home security systems. Artificial intelligence plays a role in home security, mostly through biometrics identification and verification.

Biometric Technology in Home Security

The concept of biometrics has been known for thousands of years. The history of biometrics can be dated back to 200 BC in China and 500 BC in Babylon in cases where fingerprints were used in business dealings. Besides these, there have been further records of the growing interest of people in the subject of biometrics through the years. Dating from the fourteenth century, there has been growing attention in the area of friction ridge skin (skin of the palms, fingers, toes, and soles of the feet). A Persian book of the time known as "Jaamehol-Tawarikh" suggested that fingerprints be used as a means of identification. Further research of the friction ridge skin would follow and in the year 1788, an anatomist Dr. Mayer discovered that the pattern of arrangement of friction ridge skin could never be replicated in any two people, and as such, everyone has a unique arrangement of ridge skin, nevertheless there could be similarities but never exactness. There were other papers and books describing the ridged skin before these.

It was not until the 19th century that the first biometrics systems for identification were developed. A French man known as Alphonse Bertillon developed an identification system to identify criminals. It was a technique that involved the measurement and recording of different parameters of the body parts, including height and arm length. Measurements were recorded on cards known as anthropometrics/Bertillonage. Later on, a British officer named "William James Herschel" would use fingerprints as a form of surety, making his subcontracts sign contracts with their fingerprints to guarantee that they could be found should they welsh.

Around the 1880s, a new method for identification using fingerprints was discovered, it was called the Henry classification System. This system was developed to be used in the police force by Sir Edward Henry, Sir Francis Galton, and Azizul Hague. It was a more efficient

identification system than anthropometrics and data could be easily managed (stored, classified, and retrieved) in this system. This idea paved the way for the fingerprint system later used by the FBI and the fingerprint branch at the new Scotland yard (metropolitan police). The henry system would later bring about the question of what other unique characteristics of the human body could be used for identification. This idea led to lots of research being carried out and advancement in the field of biometrics. In 1936 the concept of using the Iris as a means of Identification was proposed and in the 1960 s a semi-automated face detection system was developed. However, this system was manual as it required that the operator be mapped out and extracted facial features with which calculations were done to determine identity. Woodrow W. Bledsoe developed this system. In 1965 the first signature recognition system was built and in 1994 the first iris recognition system was developed and patented. As such, much more advancement was made in the field through the years to this current century.

At the beginning of the 21st century, great feats had been achieved in the field of biometrics, and efficient working recognition systems had been developed. Biometrics systems could now be sold commercially on a small scale for numerous uses and the United States had awarded several patents for these discoveries. Biometrics, as of today, has been integrated into almost every aspect of people's daily lives. While more advancement is still being made today, artificial intelligence is now being integrated and used for biometrics. This idea aims to create a system with the potential of learning and adapting to changes in the human body. With deep learning, more efficient systems are being created for identification. Today, almost every human body parameter can be measured with some kind of biometrics system for either identification or authentication (as used in mobile phones).

Biometrics describes the calculation and measurement of unique features of a person's body like a fingerprint, eye, face, veins, odor, etc. With this, a person can be identified. Biometrics technology is utilized for either identification or authentication. In the case of identification, an effort is being made to discern a person's identity. Whereas for authentication, a person's identity is verified by contrasting a biometric feature to a set of stored biometric templates.

There are two categories of biometrics. Physiological measurements include fingerprints, face shape, iris, retina, hand shape, veins, etc. Behavioral measurements include signature dynamics, keystroke dynamics, gait, voice recognition, gesture, etc. Biometrics has found applications in numerous sectors, ranging from airports to hospitals, banks, mobile phones, attendance, and security. Efforts are still to advance this field of technology.

Face recognition is usually done by detecting faces in either the image or video, extracting them, and then comparing them against a set of face data in a database to verify a person's identity. Although no facial recognition technology is 100% efficient, it has still found widespread application because it does not require contact and is non-invasive. However, there are a few factors that can affect the precision of a face recognition system, including lighting, varying facial expressions, and image resolutions. However, certain measures can be taken to control these factors to a certain degree and get better recognition accuracy. Face recognition has found applications in mobile devices, robotics, forensic analysis, law enforcement, security, advertising, etc.

Face detection and recognition is the biometrics technology chosen for the suggested PHSS. Based on the setting (environment) and economic instability for low-income earners, the PHSS is succinct as burglars or criminals would not intentionally place their hands on a fingerprint device to be identified by it.

Unmonitored Security Systems

These systems consist of motion, door, and glass-breaking sensors to detect intrusion and set off a loud alarm should an intruder be detected and they aren't built to notify homeowners or the police of such incidence. The advantages of using these systems are that burglars or intruders can be scared off a property and they are cost-effective. Challenges associated with using these systems are that they are not very effective when the homeowner is away and there are no neighbors around.

Monitored Security Systems

These systems are mostly designed with motion sensors, cameras, door sensors, glass-break sensors, and alarms. They do more than just set off alarms when an intruder or break-in is detected. They either notify the homeowner, police, or the company supervising the system. Some of the challenges associated with these systems are power outages, costs, and false alarms.

Wireless security systems could be set up as monitored or unmonitored security systems wirelessly. It is easy to install and more cost effective than wired systems and relies more on batteries as a power source. However, they are susceptible to signal interference and hacking. These systems consist of components that are hard-wired to a control panel. Security companies that provide these types of systems use phone lines to interact with them and know the state of the homes. The advantage that wired security systems have over wireless security systems is that they are more reliable, and consistent and are less prone to interference and hacking. The challenges associated with these systems are that burglars can easily disarm them by cutting the phone lines and they are more expensive and difficult to install.

Another method is 'face detection', while this is not the most accurate biometrics technology, it is, however, the fastest growing and can be placed in the top three. The origin of face recognition dates back to the 1960 s when

Woodrow Wilson Bledsoe developed a semi-automated system for face detection. This system was manual and used a device called a RAND tablet. The device was used as an input device to input horizontal and veridical coordinates on a grid using a stylus that emitted electromagnetic pulses. The RAND tablet was then used to input the coordinates of features on a human face, such as the ear, nose, lips, hairline, and eye. The distance between these features was calculated. These metrics were stored in a database and whenever there was a new face image to be identified, the metrics of the face would be extracted and the system would compare it with metrics in the database and the result of this would be the most closely matched. At the time, factors such as illumination, aging, and tilting of the face affected this method, and a limitation in technology.

In the 1970 s, three men improved Wilson's system: Goldstein, Lesk, and Harmon. They improved accuracy in the system by using 21 specific markers, which included hair color and lip thickness. The automation of the system was improved, although the metrics still had to be inputted into the database manually.

A new face recognition method was developed in 1988, called the eigenface approach. It was developed by Sirovich and Kirby, although it was initially a search for low-dimensional image representation. They explained that analysis of face features done on a set of images could form a set of basic features and that not more than a hundred features are needed to accurately code a normalized face. This idea led to a significant development in the field of face recognition and as such, led to the first automated facial recognition system in 1991 by Turk and Pentland. However, still facing the challenge of limited technology and environmental factors, the Eigenface has formed the basis for lots of facial recognition algorithms today.

A program known as the FERET program was initiated between 1993 to the 2000 s as a way to encourage innovation, development of more advanced facial recognition technology and commercialize facial recognition. The program was about growing a database of facial images. As of 2003, the database had 24-bit color versions of images and had a test set of 2413 images from 856 people. During the super bowl football game held in 2002, law enforcement authorities conducted a mass test of facial recognition technology and while the test failed, it was recorded to have detected a few petty criminals. The failure of the experiment was because, at the time, face recognition technologies at the time weren't efficient when operated for large crowds. However, this didn't see the end of facial recognition in the security sector as facial systems were further installed tactfully to identify criminals. Later on, Facial Recognition Vendor Tests (FRVT) were designed as a way of evaluating all existing facial recognition systems in the United States, both commercially sold and prototyped. Results of the evaluation were made available to law enforcement agents and the United States government for the implementation of better recognition systems.

More advancements and improvements were made in the facial recognition field and more algorithms were created. It started gaining more use for law enforcement and in 2009, a forensic database was designed and it allowed officers to access image records of the department of highway safety and motor vehicles. After this, officers would carry cameras so as to take pictures of suspects and compare them with images in the database. This aided investigations and the arrest of criminals. Face recognition has now experienced widespread applications. Some relevant applications of facial recognition in recent years are in 2010; facebook implemented facial recognition as a way of identifying faces featured in images uploaded. Also in 2011, face recognition was experienced in the first major installation in an airport. The same year, Osama Bin Laden was identified using facial recognition and in 2017 apple adopted the use of face recognition for mobile phone security. This field keeps advancing and its full potential and relevance are yet to be attained.

The objective of face detection is to locate and extract all faces in images regardless of their orientation, position, lighting conditions, pose, and scale (Yang and Ahuja, 2001). Face detection methods can be divided into four i.e., knowledge-based method, feature-invariant method, template matching method, and appearance-based method.

The knowledge-based method is based on obtaining the knowledge we (human beings) have about faces and translating them into rules. Common rules are that a face consists of two symmetrical eyes, a nose, and a mouth that are certain distances from each other. The challenge with this method is the difficulty associated with building a suitable set of rules. This is because if too much information was provided, there would be too many false negatives and if the rules were too generalized, there would be too many false positives. A solution to this challenge would be to build hierarchical knowledge-based methods (Solanki and Pittalia, 2016). The feature-invariant method recognizes faces by finding invariant features of faces despite their position or angle. It uses structural features of the face such as the chin, eyes, nose, mouth, the areas surrounding the cheekbones, the location of the nose and eyes, the sides of the mouth, and the distance between the eyes (Solanki and Pittalia, 2016). This method seeks to overcome the constraints of the knowledge-based method (De Carrera and Marques, 2010).

The template matching method compares input images with stored parameterized face templates. It tries to define a face as a function. Distinct features on a face can be defined separately. Edges can also be used to build the face model and shapes can be used as a representation of a face. The limitation of this method is to frontal faces. Other templates use the relation between face regions in terms of brightness and darkness. Detection is done by the

correlation between these standard patterns and input images. This approach has simple but is not sufficient for face detection. It cannot achieve satisfactory outcomes with contrast in scale, shape, and pose (Solanki and Pittalia, 2016). The appearance-based method relies on machine learning and statistical analysis to find suitable features of a face. (Solanki and Pittalia, 2016). The appearance-based holistic method (briefly discussed above) and the local appearance-based method (Ekenel and Stiefelhagen, 2006). A local appearance-based method is a geometrical approach otherwise known as a feature or analytic technique. The Local binary pattern can be used with the local appearance-based method for feature extraction. It is a texture technique used to extract features from objects. The local binary pattern is defined in a 3×3 matrix which is shown with the following equation (Kortli *et al*., 2020).

$$LBP = \sum_{p=1}^{8} 2^{p} s\left(i_0 - i_p\right), with\, s(x) = \begin{Bmatrix} 1 & x & \geq 0 \\ 0 & x & < 0 \end{Bmatrix} \quad (1)$$

Feature Extraction Techniques in Face Recognition

Feature extraction is the process of extracting relevant face component features from a human face image (Benedict and Kumar, 2016). There are several steps involved in feature extraction, which can overlap. These steps are dimensionality reduction (which could be the result of feature extraction and selection algorithms), feature extraction, and feature selection. Both algorithms could also be defined as cases of dimensionality reduction (De Carrera and Marques, 2010).

As previously stated in 1.1.5, face recognition is simply the identification of a face from a video or image. Its advantage over other biometrics technology is that it has high accuracy in addition to low intrusiveness (Lin, 2000). The following three methods are used for face recognition (Parmar and Mehta, 2014).

- Holistic matching methods
- Feature-based (structural) methods
- Hybrid methods

The holistic matching method is also called the appearance-based method. It uses the entire information of a face patch and then performs some transformation on the face patch to get a compact representation for recognition (Zhao *et al*., 2003). Examples are eigenface, linear discriminate analysis, ICA, and PCA (Parmar and Mehta, 2014). Feature-based methods occur when commonly observed features such as nose, mouth, and eyes are extracted and their locations and local statistics (geometric and/or appearance) are fed into a structural classifier. A big challenge for this method is feature restoration. This process occurs when the system attempts to retrieve invisible features due to significant variations (Parmar and Mehta, 2014). The hybrid method combines the other two methods above. It uses 3D images. A face is caught in 3D which allows the system to note the curves of the eye socket or shapes of the forehead and chin. Even a face in profile would serve because the system uses depth and an axis of measurement, which gives it enough information to construct a full face (Parmar and Mehta, 2014).

Challenges of Face Recognition Algorithm and Improvements

Although face recognition has many proposed face recognition algorithms and has demonstrated good potential, the task of robust face recognition is still difficult and face recognition techniques have several problems (Kurmi *et al*., 2014). Changes in illumination affect the shading and shadow visibility in images and the intensity of light bouncing off an object. Variations in illumination can also result in facial images of the same person appearing different, which could make as large a difference as when the identities or viewpoints are changed. (Solanki and Pittalia, 2016). Also, camera characteristics and internal camera control can affect the appearance of the face to a certain degree. The problem of lighting/ illumination is considered the major problem faced by system designers when designing a highly efficient face recognition system. Lighting and illumination are such a challenge wherein the images of the same person can appear dramatically different (Hassaballah and Aly, 2015).

Pose variations of faces in images in a challenge in face recognition. Face recognition systems can tolerate cases with small rotation angles, but some facial features may become partially or wholly occluded as the angle goes higher. Pose variation could make it more challenging for face recognition systems due to projective deformations and self-occlusion. In situations where the database might have only frontal views of faces or rely on a single-point view, there could be faulty recognition or no recognition at all (Solanki and Pittalia, 2016; Hassaballah and Aly, 2015). Facial expressions change the appearance of a face. Also, facial hairs such as mustaches and beards can alter facial appearance and features in the lower half of the face. Hairstyle and make-up could also change the facial appearance or hide some facial features. This feature makes it hard for the recognition system to accurately match the faces with faces stored in a database. (Hassaballah and Aly, 2015; Kurmi *et al*., 2014).

Occlusion means partial blockage of a face image by an object. This process makes it difficult for faces to be detected and even when faces are detected, accurate face recognition might not be possible (Hassaballah and Aly, 2015). Aging is a natural process in which the features of a human face change with time. Aging and wrinkles could cause a huge problem for face recognition; its effects are not generally researched in face recognition. A reason for

this would be the low quality of old images and the absence of a representative public database with images of people of different ages in their lives. In this case, challenges associated with aging and wrinkles could be solved for an individual if there was a dataset of the face images of that person taken at different stages of the person's life. However, this is very difficult (Hassaballah and Aly, 2015).

Remote Techniques for Data Distribution and Management

For this PHSS implementation, all faces and images captured are stored in a single database. When motion is detected and snapshots are captured, all images are sent to an API along with the homeowner's unique identification. These images and faces are then stored as belonging to that homeowner, although they are still used altogether for face recognition, even for other homes. For each set of images on getting to the API, an attempt is made to attract faces and recognize them, if a successful recognition was not made, these images are stored in a different table in the database from which the house owner where the images were taken can be prompted through a web interface to provide identification for the faces if possible. If a successful identification was made, the faces can then be added to the table of known faces and further presented with the identification provided. Each homeowner can only have access to images or faces captured at his/her home, although faces from all homes will be used for recognition of any face coming from any individual home. The restriction of homeowners' access to data from other homes will be ensured through proper authentication. The API at the server side will be authenticated using OAuth2 for every request from the server side to stop unauthorized access to the data in the database. Requests will also be sent through HTTPS to improve security.

Biological Explanation of Iris Technology and Face Peculiarities in Home Security Device

The iris is an externally visible, protected organ whose unique epigenetic pattern remains stable throughout adult life. These characteristics make it very suitable for biometrics identification (Olatinwo *et al*., 2013). Iris patterns were first proposed as a basis for personal identification by French ophthalmologist Alphonse Bertillon. However, Cambridge researcher John Daugman implemented a working automated iris recognition system in the nineties for the first time. The Daugman system is the most popular and successful system, but other systems have also been developed over the years. The Daugman system is patented and the rights are now owned by the company Iridian technologies (Matin *et al*., 2016; Olatinwo *et al*., 2013).

Iris recognition has the highest proven accuracy and has no false matches in over two million cross-comparison. It is also unique because no two irises are the same, just like fingerprints (although the amount of information that can be measured in a single iris is much greater than in fingerprints). There is no detailed correlation between the iris patterns of even identical twins or an individual's right and left eye. Iris recognition allows high-speed processing and an individual is only required to look into the camera for a short time. The iris is less susceptible to spoofing, is stable for an individual through his or her lifetime, and does not change with age (Dias *et al*., 2010). Unlike the human face changes and wrinkles with aging. However, this PHSS uses face recognition because it is less intrusive.

Researchers have explicitly explained the steps involved in iris recognition (Khanam *et al*., 2019; Olatinwo *et al*., 2013; Matin *et al*., 2016; Dias *et al*., 2010), including image acquisition image pre-processing, segmentation, normalization, and feature extraction and matching. Image acquisition is the first step in image processing. It captures a high-resolution digital image of the eye normally with a high-resolution camera with an infrared illumination facility. High-quality acquisition techniques are used for iris recognition to make accurate models of different surfaces. Image pre-processing is aimed at enhancing the ability to quantitatively interpret image components. It removes low-frequency noise, normalizes the intensity of individual images, and removes reflections. Segmentation simply has to do with isolating the iris region from an input image. The iris region can be approximated by two circles, one for the iris/sclera boundary and another, interior to the first, for the iris/pupil boundary. Once the iris region is successfully segmented from an eye image, the next stage is to transform the iris region to have fixed dimensions to allow comparisons. The normalization methodology will create iris regions with the same measurements, so two photos of the identical iris under exclusive conditions will have characteristic features in the same spatial area. A technique based on Daugman’s rubber sheet model can be employed for the normalization of iris regions. The pupil's center can be considered the reference point and radical vectors pass through the iris region. The virtual circles technique can also be employed. The template that is created in the feature encoding procedure will require a relating matching metric, which allows comparison between two iris templates. Matching can be done using Hamming distance. Other techniques are weighted Euclidean distance and normalised correlation.

Reason for Using Face Recognition Instead of other Biometrics Techniques

In this case, other biometrics techniques include fingerprint recognition, voice recognition, IRIS recognition, and RFID cards. While most of these biometrics techniques have higher accuracy than the face detection and recognition technique, they are unsuitable

for surveillance and monitoring. More so, its affordability has a significant role in its patronage as the essence of this review is to seek ways of reducing crime in a low-income home environment. Hence, its affordability is also tied to high maintenance costs and higher energy consumption. Comfortability is another essential part of homes that can afford newer technologies. For example, the convenience of getting the fingers of visitors on a fingerprint machine is significantly low and embarrassing. Also, it is time-consuming to scan fingerprints on visitors' glass cups. The same disadvantages apply to the IRIS technique as capturing the IRIS of each person might not be so possible. Also, the voice recognition system would be no different from cases of visitors with voice impairment. Hence, the need for a system similar to the human eye is what the face detection and recognition system offer. This system makes the most sensible and recommended face detection and recognition technique based on affordability and comfortability.

Designing a Home Security System

"Design and implementation of smart home security system" by Hossain *et al*. (2014) is a smart home security system that's designed for homes and focuses on reducing the rate of burglary occurrences through the use of automation rather than just the traditional doors and locks that can be easily broken into. This research utilized a Near Field Communication (NFC) tag card and shield, Keypad, and PIR motion sensor for input and an LCD display, Buzzer alarm, and servo motor for output. Also, a Peripheral Interface Controller (PIC) microcontroller 16F877A and an Arduino Uno for power supply were used for hardware implementation. Figure 2 shows the block diagram of the project.

Here the Arduino provides a power supply to the servo motor and the PIC provides PWM (Pulse Width Modulation) signal to operate the servo motor. Hence both an NFC tag card and password must be provided for the door to be unlocked. If only an NFC card is provided, the servo motor gets power from the Arduino but no PWM from the PIC, and vice versa if only the password is provided. Password is stored in the EEPROM of the PIC. When a person enters a password, it is decoded and verified against the stored password. If the password is correct, the PIC sends a signal to the servo motor. When the NFC card is placed near the shield and matches, the Arduino sends a signal to the base of the NPN transistor, which acts as a switch. When it receives a signal at its base, it connects the servo to the power supply. A PIR motion sensor is placed in the room and when motion is detected, the buzzer is set off. The PIR motion sensor is switched off on successful authorization from both the NFC shield and keypad lock password. When the user leaves the room, the PIR sensor can be switched back on by placing the NFC card at the shield and pressing C on the keypad. Also, the password can be changed only by the authorized user. In summary, a room is guarded by placing a PIR motion sensor which sets off an alarm if an unauthorized person gains access to the room. The authorization is granted by the use of an NFC card and shield and a keypad lock. Both an NFC card and the correct password must be provided to gain access to the room.

Another novel design for home security is the "development of gsm-based advanced alert home locker safety security system using Arduino UNO" (Murthy *et al*., 2018). This design is similar to the aforementioned research above, in the sense that it requires two factors to authorize a user to access a room. However, in place of an NFC shield and card, a fingerprint scanner is used alongside a keypad to input passwords. This design utilizes a fingerprint module, driver unit, motor, keypad, multiplexed seven-segment display, GSM module sim900A, buzzer, and Arduino UNO for its implementation. Figure 3 shows the block diagram of the project.

When a user places his finger on the fingerprint module, it scans it and compares it with the already stored fingerprint. If it matches, the user can then go on to input the password in the keypad. If fingerprint verification fails, the buzzer is set off and a message is sent to the homeowner, alerting him/her of a possible intruder. On successful verification of fingerprint, but wrong input of a password, the buzzer is also set off and the homeowner is notified through his/her GSM. If both verifications are successful, the motor is rotated clockwise and the door is opened, allowing access to the user.

Also, "design and development of home security systems based on internet of things via favourite platform" (Abu *et al*., 2018). This design utilizes IoT to ensure real-time home surveillance. Components used in this research are a PIR sensor, IR sensor, Blynk application, espresso lite V2.0 as the microcontroller, OLED display and setup communicates with an online webserver which is favourite. Figure 4 shows the block diagram of the design.

The Espresso Lite is connected to a UC00A which supplies a voltage of 3.3v to the board. The microcontroller connects to the internet through an internal Wi-Fi board (ESP-WROOM02). The two sensors supply the input to the setup and the data is then sent to the Favoriot web server, which in turn notifies the homeowner. The system will only work in the absence of the homeowners and can be turned off and on using the Blynk application. The OLED is used to display data. On start-up, the system connects to Wi-Fi and Blynk and the OLED displays the status of the connection. The Blynk virtual switch is then used to turn on or off the system for which the OLED will indicate a status. Inputs from the sensors will then be read. If the motion is detected, the OLED displays an output based on data from the sensors. The input data from sensors will then be sent to the server and stored in the data stream and the graph will automatically be plotted and then alerts will be sent to the user from the server.

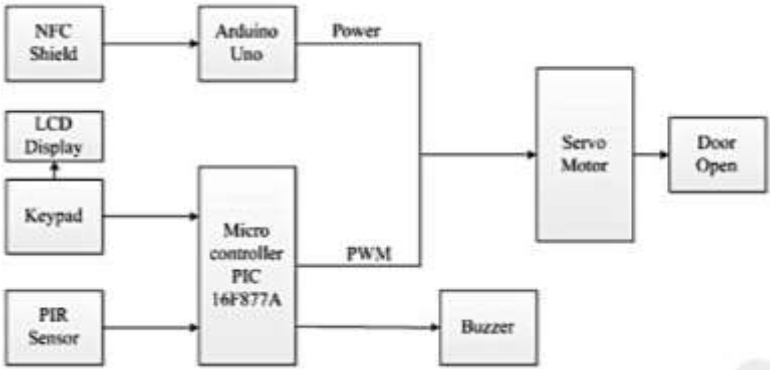

Fig. 2: Block diagram of "design and implementation of smart home security system" (Hossain *et al*., 2014)

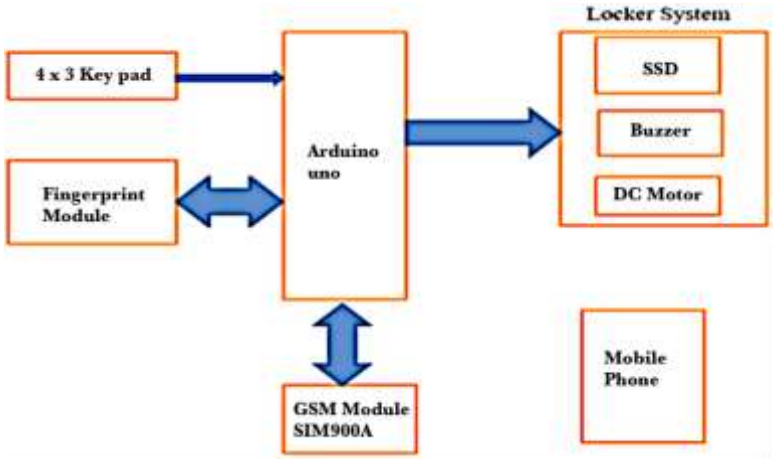

Fig. 3: Block diagram of "development of GSM-based advanced alert home locker safety security system using Arduino UNO" (Murthy *et al*., 2018)

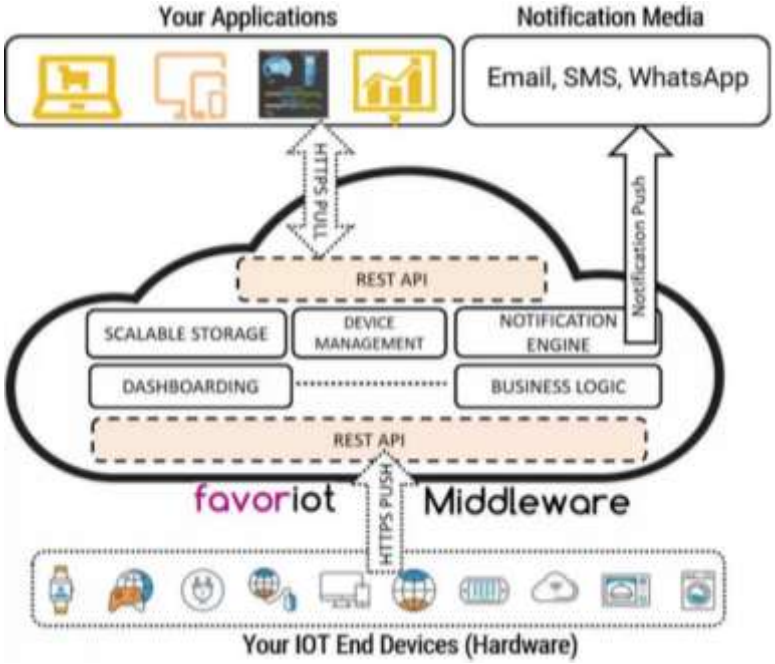

Fig. 4: Block diagram of internet of things enabled home security systems (Abu *et al*., 2018)

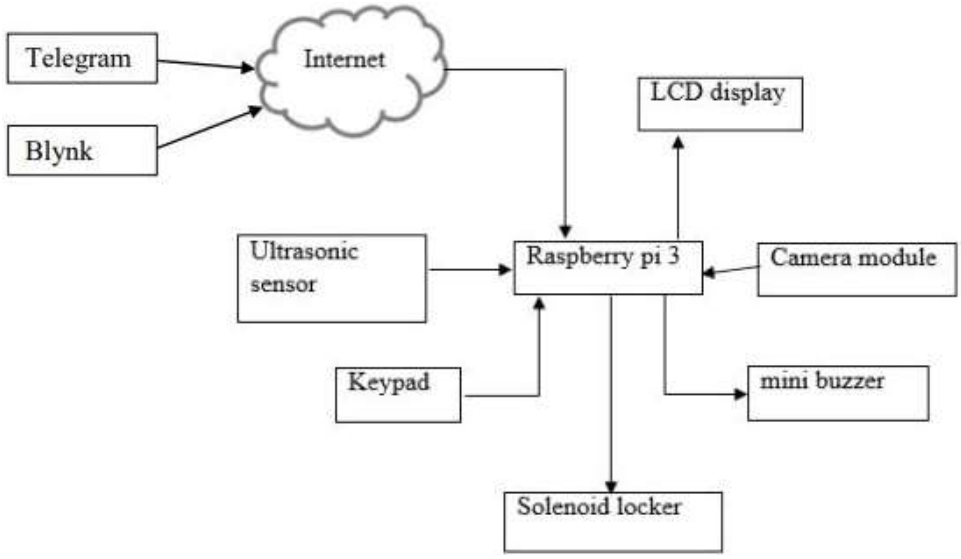

Fig. 5: Block diagram of the "anti-theft security system using face recognition design" (Chong *et al*., 2018)

In addition, "anti-theft security system using face recognition" (Chong *et al*., 2018). The research uses the following software and libraries: Blynk, telegram, python, and OpenCV. And makes use of the following hardware: A raspberry pi 3 model B, solenoid electric door locker, a keypad, a 1602 LCD display, an ultrasonic sensor module, a camera module, and a mini buzzer. Comparing this system to the proposed home security system in this write-up, it is a very similar security system that implements most of the concepts the same way. The "anti-theft security system using face recognition" design functions by using an ultrasonic sensor to detect the presence of a person, after which a camera is triggered to capture the person and compare his face with faces in a database (this database is restricted to a particular system, each system having a separate database). If the person is unable to be identified, a buzzer is set off and the person's face is sent to the house's owner via telegram. However, if the face is recognized, the person needs to put the correct password into the keypad to unlock the solenoid locker.

An improvement to this design would be to make each system communicate with a central database to ascertain treat levels of people assessing each home. Sharing information between each system and a central database would better inform homeowners of real security threats, rather than just setting off a buzzer each time a face is not unidentified. Figure 5 shows the block diagram of the project.

Finally, "Design and Implementation of Home security system using Zigbee and Arduino controller with sensors" (Abdulqader, 2019). This research uses a PIR sensor, a gas sensor, an Arduino Uno board, an NTC thermistor sensor, a buzzer, a hex keypad, a Bluetooth module, and Zigbee. When motion is detected from either doors or windows in this design, the buzzer is set off.

The disadvantage of this design implementation is that irrespective of who or what is detected, the buzzer goes off. The house owner had no way of knowing who or what caused the motion. Furthermore, even in cases where the house owner is responsible for the motion, the alarm is set off. The alarm will be set off unnecessarily and will eventually be inconvenient. This design can be improved by including a camera or face recognition interface making it a smart system capable of telling what is responsible for detected motion and in more advanced levels, it can identify who or what it is.

Propose Design of a Low-Cost Home Security

The first requirement is the design of a low-cost security system. Hence, the construction requires the list of components, frameworks, or software used as follows:

- Microchip's PIC16F877A as the main controller
- LM339 as sensor interface
- UM3561 is a tone generator
- µPC2002 as a speaker driver (audio amplifier)
- LM7805, LM7812 and LM317 voltage regulators are used to obtain +5V, +12V and +3V respectively
- HC-SR501 PIR Sensor/Motion sensor

Languages, frameworks, and software used are:

- Raspbian OS
- Python IDE
- NET framework (using ASP.NET Web API and C #)
- OpenCV/EmguCV
- Typescript
- Angular

When these components are connected as presented in Fig. 6. Then IC1, IC2, IC3, and IC4 are removed from the IC bases. A voltage of 18 to 22 V max. DC source is applied to the power connector (J3). Ensure that the voltage between Pin12 (GND) and Pin3 of IC2 is between 4.8-5.1 V DC. Also, the voltage between GND and E$4 jumper should be between 11.7-12.3V DC. The voltage between Pin1 and Pin3 (GND) of JP1 should be between 2.5-3.1 V. If the above measurement is ensured, then disconnect the power supply and insert IC1, IC2, IC3, and IC4 into the appropriate IC bases. Then attach all the other sensors as in the initial design. The IoT-enabling sensor is important to ensure compatibility with a smartphone. The programming code using the languages alighted above is used to insert the necessary protocols. The incorporation of the database is included in the storage protocols to enhance the retrieval of data by facial similarities. The imagery protocol can be adapted from Guo *et al*. (2016).

The power source has a 5 v and 2 A raw voltage input with a Broadcom BCM2837 64bit Quad Core Processor that operates at a voltage of 3.3 v. Each input/output pin operates at a current of 16 and totals 54 mA for all pins and can operate at temperatures between -40 to + 80 c. Its camera weighs 0.9 kg while yet providing powerful capabilities. It has a still resolution of 1280 × 720 with 5mega-pixels and HD video standards. It has a 30 fps frame rate.

HC-SR501 PIR (Passive Infrared Sensor) is basically a sensor used to detect the motion of objects. It simply works by detecting radiant heat emitted from an object. It measures the room temperature and works by detecting any change in the surrounding heat emitted. The PIR sensor uses a pair of sensing elements, such that each sensing element is sensitive to infrared rays. When there is no motion, the two sensing elements detect the same amount of infrared present in the room or being emitted from a nearby wall or door. When an object passes the sensing area, assume this to be a human being or animal, it obstructs the infrared, which was already being detected by the sensing elements. The object is detected first by one of the sensing elements, which causes a positive differential change between the two sensing elements and when the radiating body leaves the sensing area, there is a negative differential change. The PIR detects motion using these changes in pulse. An illustration of how the PIR motion sensor is shown in Fig. 7.

The two sensing elements are enclosed imperviously in metal to protect the sensors from humidity, noise, and temperature. There is a small window on the top; it is made of an infrared transmission material. Coated silicon is commonly used for this. The sensors used in the PIR motion sensor are made of pyroelectric crystals and a Fresnel lens is used to widen the sensor's range. The HC-SR501 PIR Sensor is shown below in Fig. 8.

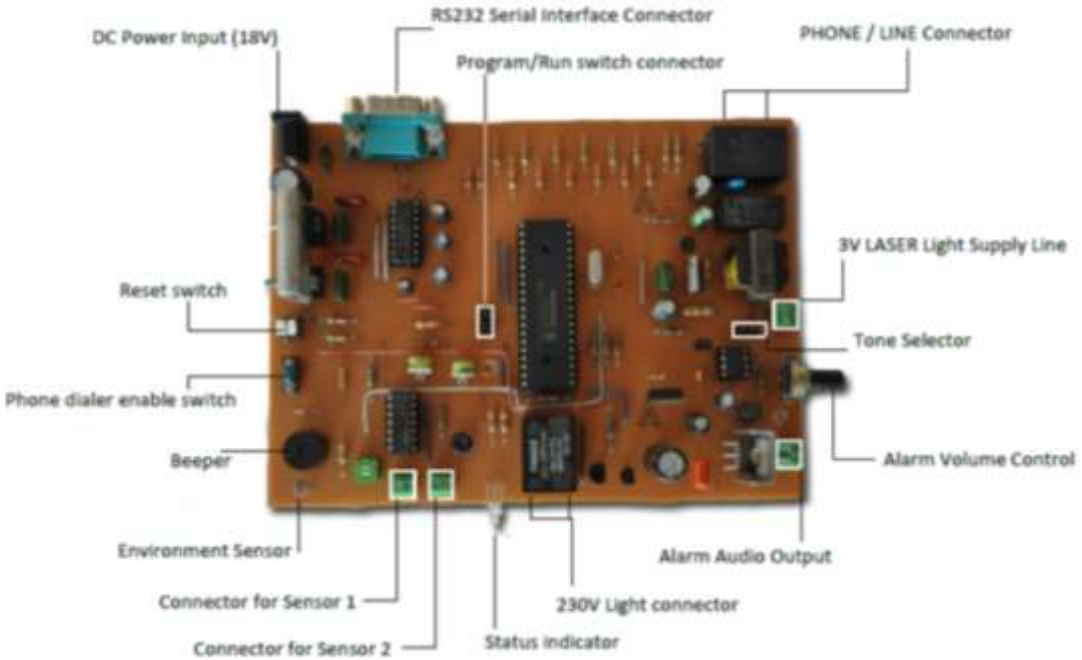

Fig. 6: Low-cost home security design (Dilshan, 2022)

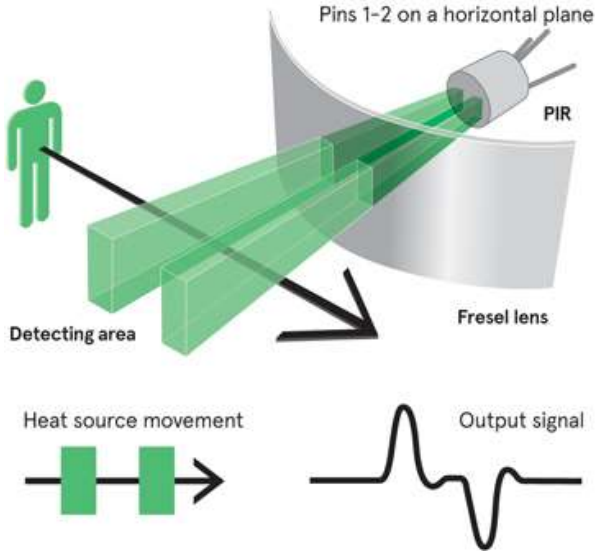

Fig. 7: Illustration of how a PIR sensor works (Keenan, 2018)

Fig. 8: HC-SR501 PIR sensor (Adafruit, 2020)

The PIR motion sensor operates using the input pin (VCC), output pin (Dout), and ground. It also uses a sensitivity control and an off-time control. The sensitivity control is used to increase the sensor's sensitivity; it increases the range the sensor should cover. While the off-time control is used to set the time for how long the output signal should remain high. It operates in two modes: Repeatable (H) mode and non-repeatable (L) mode. When the sensor is in this Repeatable (H) mode, the output (Dout) will signal when motion is detected, but the sensor will, however, continue giving out a high signal even when the motion can no longer be detected. Non-repeatable (L) mode: When the sensor detects motion in the mode, it gives out a high signal and continues the signal as long as motion can still be detected. The output becomes low when the motion can no longer be detected (the high signal stops being outputted depending on the time set with the off-time control).

Face Recognition Libraries/App/Software for a Simple Home Security System

The apps or software discussed in this section include .Net Framework (using ASP.NET web API and C #), C # scripts, ASP.NET app, OpenCV software, EmguCv app, Accord.Net Framework, and Angular web app. '.Net' pronounced as "dot net" is a software development platform made up of tools, programming languages, and libraries to build many different application types. There are different implementations of the .NET framework. These various implementations allow .NET to execute in different platforms-macOS, Windows, Linux, iOS android, etc. C# pronounced as "see sharp" is a general-purpose, object-oriented programming language that has roots in c, c++, and java, with the objective of combining the power of these languages with the ease of visual basic. It is appropriate for creating demanding applications on a large scale like enterprise applications, web-based applications, mobile applications, and cloud-based applications.

ASP.NET is a web development framework built within the .NET framework for creating dynamic web pages. It has tools and libraries to aid programmers in building web applications and services. It was built to modify the active server page technology and was released in 2002. Features of the ASP.NET framework include an authentication system, editor extension, and libraries for common web patterns. This design uses a web application built on the ASP.NET web API framework to receive HTTP requests from the raspberry pi and then do all necessary data storage and processing. ASP.NET web API is a framework that is used for building HTTP services that can be accessed from various platforms; an example is the raspberry pi used in this design. It uses HTTP requests to communicate and send data to clients. It uses controllers to process requests. HTTP stands for hypertext transfer protocol and facilitates communication between server and client. It is a client sending a request to a server which the server processes and sends a response in return. Commons HTTP methods are used to get, post, put and delete. A 'get' request is used to request/retrieve data from the server. It is the most common request used. A 'post' request sends data over to the server from the client side. A 'put' request is commonly used to update/modify data on the server. A 'delete' request is used a delete specific data or information on the server side.

Open-source computer vision library is a collection of programming routines, methods, or functions for computer vision. It integrates functions for image processing with machine learning. It is a library consisting of classic and ultramodern computer vision and machine learning algorithms to enhance computer vision applications and encourage machine learning technologies for commercial products. The functionalities of this library range from object identification, face detection, and recognition, classification of human actions in videos, tracking moving objects, finding similar images from an image database, following eye motion and tracking camera motion, extracting 3D representation of objects, and much more.

OpenCV has been employed by giant companies like Intel, google, Toyota, IBM, Yahoo, and microsoft. Examples

of some of its use cases are monitoring equipment in China, aiding robot navigation, and detecting drowning accidents in swimming pools, for surveillance. Etc. It has python, java, c++, and mat lab interfaces and supports android, windows, Linux, and macOS. EmguCV is a .NET wrapper for OpenCV. It enables OpenCV functions to be used in the .NET environment. EmguCV is required because .NET is an interpreted environment and hence, .NET languages cannot directly call OpenCV functions written in C/C++. EmguCV is also cross-platform and is employed in this design for face detection and recognition.

Accord .Net is a .Net framework for scientific computing. It can be used for machine learning, artificial neural networks, statistics, image processing, signal processing, numerical linear algebra, and numerical optimization. Angular (also known as angular 2+) is a typescript client-side web application framework. It is open source and was developed by Google as a rewrite of angular JS. It will be used to build a web-based interface to interact with the system in this design.

Conclusion

From this review, it is clear the more reasonable way of curbing insecurity in a community is to go to the basis, i.e., the home system where everyone interacts with his neighbor or friends. Hence, the minimum requirement for patronage of a home security system is affordability and comfortability. To a low-income earner, it is easy to tie affordability to his/her inability to accommodate the cost of purchase, maintenance, and upgrade of technology. So why must a low income stay with more accurate biometrics such as fingerprint recognition, voice recognition, IRIS recognition, and RFID cards when he cannot meet basic face recognition? To an average income earner that could afford newer technology, it becomes a social burden to get visitors' fingers on a fingerprint machine and time-consuming to scan fingerprints on visitors' glass cups. The same disadvantages apply to the IRIS technique as capturing the IRIS of each visitor might not be convenient for all. Also, the voice recognition system would be no different from cases of visitors with voice impairment. Hence, the need for a system similar to the human eye is what the face detection and recognition system offer. This makes the most sensible and recommended face detection and recognition technique based on affordability and comfortability.

In this write-up, an affordable and comfortable home security system was suggested. The different specifications based on likely users' demands were documented. This system is believed to have 68% accuracy, which may be basic to connecting individual security architecture to a shared central database. This suggestion meets the basic requirement to curb crime to almost 65% in any community, village, or town when at least half of its population could afford a home security system. Hence, based on the concept of affordability and comfortability, the suggested home security is highly recommended to governments and policymakers.

Acknowledgment

The authors appreciate host institutions for their partial sponsorship.

Funding Information

This project received no funding. Special appreciation to Bowen University Nigeria for paying the APC.

Author's Contributions

Moses Eterigho Emetere: Conceptualize the work, supervised the construction and wrote part of the paper.

Daniel Chidera Okpala: Construction of the device and wrote part of the paper.

Muhammad Muhammad Bakeko and Sunday Adeniran Afolalu: Wrote part of the paper.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Abu, M. A., Nordin, S. F., Suboh, M. Z., Yid, M. S. M., & Ramli, A. F. (2018). Design and development of home security systems based on the internet of things via favoriot platform. *International Journal of Applied Engineering Research, 13*(2), 1253-1260.

Abdulqader, M. F. (2019). Design and Implementation of Home Security System Using Zigbee and Arduino Controller with Sensors. *Kirkuk University Journal-Scientific Studies*,14, 34-55.

Adafruit. (2020). PIR Motion Sensor Tutorial. https://www.instructables.com/id/PIR-Motion-Sensor-Tutorial/

Al-Ali, A. R., Rousan, M. A., & Mohandes, M. (2004, April). GSM-based wireless home appliances monitoring & control system. In *Proceedings. 2004 International Conference on Information and Communication Technologies: From Theory to Applications, 2004.* (pp. 237-238). IEEE. https://doi.org/10.1109/ICTTA.2004.1307712

Ashby, M. P. (2017). The value of CCTV surveillance cameras as an investigative tool: An empirical analysis. *European Journal on Criminal Policy and Research*, *23*(3), 441-459. https://doi.org/10.1007/s10610-017-9341-6

Bangali, J., & Shaligram, A. (2013). Design and Implementation of Security Systems for Smart Home based on GSM technology. *International Journal of Smart Home*, *7*(6), 201-208. https://doi.org/10.14257/ijsh.2013.7.6.19

Benedict, S. R., & Kumar, J. S. (2016, October). Geometric shaped facial feature extraction for face recognition. In *2016 IEEE International Conference on Advances in Computer Applications (ICACA)* (pp. 275-278). IEEE. https://doi.org/10.1109/ICACA.2016.7887965

Chong, S., Dugast-Darzacq, C., Liu, Z., Dong, P., Dailey, G. M., Cattoglio, C., ... & Tjian, R. (2018). Imaging dynamic and selective low-complexity domain interactions that control gene transcription. *Science*, *361*(6400), eaar2555. https://doi.org/10.1126/science.aar2555

De Carrera, P. F., & Marques, I. (2010). Face recognition algorithms. *Master's thesis in Computer Science, Universidad Euskal Herriko*, *1*. https://www.ehu.eus/ccwintco/uploads/d/d2/PFC-IonMarqu%C3%A9s.pdf

Dias, U., Frietas, V., Sandeep, P. S., & Fernandes, A. (2010). A neural network based iris recognition system for personal identification. *ICTACT Journal on Soft Computing*, *1*(2), 78-84. https://ictactjournals.in/paper/IJSC_V1_I2_3_78_84.pdf

Dilshan, R. J. (2022). Programmable Home Security Alarm System, https://www.electronics-lab.com/project/programmable-home-security-alarm-system/

Doknić, V. (2014). Internet of things greenhouse monitoring and automation system. *Internet of Things: Smart Devices, Processes, Services*. http://193.40.244.77/idu0330/wpcontent/uploads/2015/09/140605_Internet-of-Things_Vesna-Doknic.pdf.

Ekenel, H. K., & Stiefelhagen, R. (2006, June). Analysis of local appearance-based face recognition: Effects of feature selection and feature normalization. In *2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)* (pp. 34-34). IEEE. https://doi.org/10.1109/CVPRW.2006.29

Fornasier, M. D. O. (2020). The applicability of the Internet of Things (IoT) between fundamental rights to health and to privacy. *Revista de Investigações Constitucionais*, *6*, 297-321.

Guo, Y., Lei, Y., Liu, L., Wang, Y., Bennamoun, M., & Sohel, F. (2016). EI3D: Expression-invariant 3D face recognition based on feature and shape matching. *Pattern Recognition Letters*, *83*, 403-412. https://doi.org/10.1016/j.patrec.2016.04.003

Hassaballah, M., & Aly, S. (2015). Face recognition: Challenges, achievements and future directions. *IET Computer Vision*, *9*(4), 614-626. https://doi.org/10.1049/iet-cvi.2014.0084

Hossain, M. D., Urbi, Z., Sule, A., & Rahman, K. M. (2014). Andrographis paniculata (Burm. f.) Wall. ex Nees: A review of ethnobotany, phytochemistry, and pharmacology. *The Scientific World Journal*, *2014*. https://doi.org/10.1155/2014/274905

Keenan, M. (2018). Adapting PIR sensor technology to new applications. https://www.avnet.com/wps/portal/abacus/resources/article/adapting-pir-sensor-technology-to-new-applications/

Khanam, R., Haseen, Z., Rahman, N., & Singh, J. (2019). Performance analysis of iris recognition system. In *Data and Communication Networks: Proceedings of GUCON 2018* (pp. 159-171). Springer Singapore. https://doi.org/10.1007/978-981-13-2254-9_14

Kortli, Y., Jridi, M., Al Falou, A., & Atri, M. (2020). Face recognition systems: A survey. *Sensors*, *20*(2), 342. https://doi.org/10.3390/s20020342

Kurmi, U. S., Agrawal, D., & Baghel, R. K. (2014). Study of different face recognition algorithms and challenges. *International Journal of Engineering Research*, *3*(2), 112-115. https://www.indianjournals.com/ijor.aspx?target=ijor:ijer&volume=3&issue=2&article=016

La Vigne, N. G., Thompson, P., Lawrence, D., & Goff, M. (2019). Implementing Gunshot Detection Technology: Recommendations for Law Enforcement and Municipal Partners. https://policycommons.net/artifacts/630550/implementing-gunshot-detection-technology/1611791/

Lee, L., & Cho, Y. J. (2017). The rise of artificial intelligence: What does it mean for development? https://blogs.worldbank.org/digital-development/rise-artificial-intelligence-what-does-it-mean-development

Lin, S. H. (2000). An introduction to face recognition technology. *Informing Sci. Int. J. an Emerg. Transdiscipl.*, *3*, 1-7. https://inform.nu/Articles/Vol3/v3n1p01-07.pdf

Matin, A., Mahmud, F., Zuhori, S. T., & Sen, B. (2016, December). Human iris as a biometric for identity verification. In *2016 2nd International Conference on Electrical, Computer & Telecommunication Engineering (ICECTE)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICECTE.2016.7879610

Metu, A., Kalu, C., & Maduka, O. (2018). Analysis of Crime Rate and Economic Growth in Nigeria: The Institutional Challenges and Way Forward. *Journal of Economic Studies*, *15*(1), 39-50. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386596

Murthy, B. R., Jagadish, O., Alam, K. T., Dada, V. M., & Gandhi, K. P. (2018). Development of GSM based advanced alert home locker safety security system using arduino UNO. *International Journal of Scientific Research in Science and Technology (IJSRST)*, *4*(2), 1154-1160.

Olatinwo, S. O., Shoewu, O., & Omitola, O. O. (2013). Iris recognition technology: implementation, application and security consideration. *The Pacific Journal of Science and Technology*, *14*(2), 228-33.

Parmar, D. N., & Mehta, B. B. (2014). Face recognition methods & applications. *arXiv preprint arXiv:1403.0485*. https://doi.org/10.48550/arXiv.1403.0485

Peterson, J., Sommers, I., Baskin, D., & Johnson, D. (2010). The role and impact of forensic evidence in the criminal justice process. *National Institute of Justice*, 1-151. https://www.jrsa.org/events/conference/presentations-09/Joseph_Peterson.pdf

Rani, C., Modares, H., Sriram, R., Mikulski, D., & Lewis, F. L. (2016). Security of unmanned aerial vehicle systems against cyber-physical attacks. *The Journal of Defense Modeling and Simulation*, *13*(3), 331-342. https://doi.org/10.1177/1548512915617252

Ruth, O. (2021), Nigeria: Will insecurity, kidnapping and crime get worse in 2021? https://www.theafricareport.com/58604/nigeria-will-insecurity-kidnapping-and-crime-get-worse-in-2021/

Solanki, K., & Pittalia, P. (2016). Review of face recognition techniques. *International Journal of Computer Applications*, *133*(12), 20-24.

WDI. (2016). Incidents of crime in Nigeria. https://openknowledge.worldbank.org/bitstream/handle/10986/23969/9781464806834.pdf

Yang, M. H., & Ahuja, N. (2001). *Face Detection and Gesture Recognition for Human-Computer Interaction* (Vol. *1*). Springer Science & Business Media. ISBN-10: 9780792374091.

Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: A literature survey. *ACM Computing Surveys (CSUR)*, *35*(4), 399-458. https://doi.org/10.1145/954339.954342

Zhao, Y., & Ye, Z. (2008). A low-cost GSM/GPRS based wireless home security system. *IEEE Transactions on Consumer Electronics*, *54*(2), 567-572. https://doi.org/10.1109/TCE.2008.4560131