International Journal of Information Retrieval Research
Volume 12 • Issue 1

Border Security and Surveillance System Using IoT

Siham Boukhalfa, GeCoDe Laboratory, University of Saida Dr. Moulay Tahar, Algeria

Abdelmalek Amine, GeCoDe Laboratory, University of Saida Dr. Moulay Tahar, Algeria

https://orcid.org/0000-0001-9327-7903

Reda Mohamed Hamou, GeCoDe Laboratory, University of Saida Dr. Moulay Tahar, Algeria

https://orcid.org/0000-0002-0388-1275

ABSTRACT

Security along the international border is a critical process in security assessment. It must be exercised 24-7. With the advancements in wireless IoT technology, it has become much easier to design, develop, and deploy a cost-effective, automatic, and efficient system for intrusion detection in the context of surveillance. This paper sets up the most efficient surveillance solution. The authors propose a border surveillance system. This surveillance and security system is to detect and track intruders trespassing into the monitoring area along the border which triggers alerts and valuation necessary for the catch of efficient measurements in case of a threat. The system is based on the classification of the human gestures drawn from videos envoy by drones equipped with cameras and sensors in real-time. All accomplished experimentation and acquired results showed the benefit diverted from the use of the system, and therefore, it enables the soldiers to watch the borders at each and every moment effectively and at low cost.

KEYWORDS

Barrier Coverage, Border Control, Border Patrol, Border Security System, Border Surveillance, Drone, Remote Surveillance System, Security, Security Alarm, Video Surveillance

1. INTRODUCTION AND PROBLEMATIC

The security of borders plays a key role in the assertion of national security, management of lawful immigration, prevention of smuggling, and defense against hostile threats. It is necessary to avoid hostile intrusions, the fluxes of underground immigrants, and the traffic linked by the conductors.

Indeed, borders remain the most visible mark of a state's sovereignty over a territory, and their management of its involvement in protecting its people from threats it defines as such: international terrorism, smuggling, organized crime, irregular migration, and multifaceted trafficking (human beings, drugs, raw materials or ALPC). Border threats differ from country to country, so each of the neighboring countries has developed its own structure for border guard units.

DOI: 10.4018/IJIRR.289953

However, they notice that a typical resolution for the surveillance of borders consists in putting towers of observation, of post offices of security and organizing patrols of surveillance to discern possible illegal movements of persons or vehicles in the area around border, to accomplish a big variety of missions: observation, detection and tells real-time about the slightest changeability the centers of command and control For this we propose a surveillance system to combat terrorism, smuggling, organized crime, and irregular migration, it is designed to ensure the missions of permanent control or temporary border or camp protection, bivouac, sensitive site, convoy route. The system allows continuous operation under "complex and demanding" conditions, without putting lives in danger, and which helps armies and governments to manage changes at the level of threats.

The Internet of Things (IoT) is a developing worldview that enables communication among sensors and electronic gadgets through the Internet to facilitate our lives. IoT utilize smart devices and internet to give creative answers for different difficulties and issues (Kumar and Tiwari, 2019). The structure of our system depends on connections between objects (sensors, drones, and surveillance cameras) that they give capacities to control by the center of command (which can be far from borders) before it is too late. Nature is vast, it is a powerful source of inspiration for solving complex computer problems, she always finds the optimal solution to solve her problem and maintains the perfect balance between its components, an interesting new paradigm known as the bio-inspired consists in analyzing the living world in order to translate biological models of all forms (animals, plants, micro-organisms, ecosystems... etc.) into technical and algorithmic concepts, many works have been done in the field of bio-inspiration to solve different problems and others are still in progress, the main issue in this work is the creation of a new bio-inspired technique that can enhance security while respecting the privacy of human beings represents. In this work is we use a bio-inspired model based on the style of life of the Cockroaches for the purpose of detect terrorists and non-soldier people by the characteristics of gestures which are intruders of being dangerous (criminals, terrorists… etc.) instead of the faces.

The technique is based on the connections between smart objects in which is based on picking up pictures through drones equipped with cameras that are able to connect with smartphones So that it can monitor borders from any place and the use of the characteristics of gestures that are suspected of being dangerous instead of the faces. We apply the classification of gestures human being by the Bio-Inspired technique of Grouping Cockroaches Classifier (GCC) based on the style of life Cockroaches and operate on the phenomenon of seeking the most attractive and secure place (shelter) for hiding for a good detected the gesture of unwanted individuals this algorithm is based on a learning base and classify the gestures of the test base and labels them, each gesture take one of two classes (gestures of border soldiers and gesture of terrorists and non-soldier people), and we apply also a new technology for the presentation of picture (n-grams pixels) to construct a system of control of borders. Our objective is to use drones instead of normal soldiers to cover the space of the borders, detect terrorists hiding their faces, detect people in disguise; react effectively and faster, react at night, or even when the climate is difficult. We began our work with some related works done in this field, after that in the third section we detailed description of our system, which will be followed by a presentation of experiment.

2. RELATED WORKS

In the conventional solution of controlling border traveling (that the person is eligible to enter the country and does not pose a threat to its citizens or institutions) the border guards have the responsibility for this monitoring takes place manually which are responsible for continuously keeping an eye on the borders. It takes a lot of manpower and assets as the borders are stretched across hundreds of miles and have extreme terrain as well as climatic conditions. With the improvement of document forging techniques, the uses of look-alikes and aliases, as well as the time pressure associated to border control processing, it is not surprising that border control authorities are revising the traditional manual approach and considering the deployment of the most advanced surveillance technologies to facilitate a more efficient and reliable controlling of cross-border travels.

Nowadays, several works have been done in the field of security surveillance for the border, military, and academic purposes. Palak et al (Palak and Himani, 2019) provided a survey of different Methods in Border Security and Surveillance, The aim is to compare different researches in border security. Arfaoui et al (Arfaoui and Boudriga, 2017) developed a model that estimates the crossing time of the monitored area taking into account the characteristics of the area and the behavior of the intruders crossing this area. Then they proposed a deployment method based on the intruders crossing paths that optimize the number of deployed sensors while ensuring an early and high detection level of the intruders. Laura et al (Laouira, Abdelli, 2019) proposed a multilayer hybrid architecture based on cameras, scalar sensors, radars, and UAVs to design a border surveillance system. Bhadwal et al (Bhadwal and Madaan, 2019) proposed a smart border surveillance system that can provide round the clock video surveillance at the places where human deployment is not possible. Al Abkal et al (Al Abkal and Talas, 2020) investigates the use of drones, in border security and their ability to enhance existing security measures in Kuwait's ports and borders and also along borders of the United States. The study contributes to practice by introducing the use of UAVs to enhance port security, especially for monitoring and surveillance purposes. Segireddy et al (Segireddy and Koneru, 2020) developed a light detection and ranging (LIDAR) sensor for the acquisition of distance with a range of 40 m from the position where an object resides. Data collected by the sensor is monitored and administered in a server. Software required for the analysis of data and generation of alert notifications is deployed in the server which is an added feature to the system and assists the concerned security personnel to respond quickly and engage the safety. Ayush et al (Goyal and Anandamurthy, 2020) employ machine learning techniques in Remote Video Surveillance for real-time threat level detection and classification of targets crossing borders. The algorithm used for the machine learning-based detection of objects in the videos in this research is the Viola-Jones algorithm. A threat level classifier and alert warning system were also added to classify and annotate the videos in real-time for each frame. The threat level classifier performs four-fold categorization of the real-time video into safe, low, medium, and high (danger). The alert warning system specifies the type of warning based on the type of intrusion (human, vehicle, or weapon) detected. Kim et al (Kim and Lim, 2018) propose to develop a drone-aided border surveillance system with electrification line battery charging systems (DABS-E). This paper proposes an optimization model and algorithm to schedule drone flights for a DABS-E. Through a numerical example. Karthick et al (Karthick and Prabaharan, 2019) proposed an architecture that involves a low energy intrusion detection system on the first level. If the system detects any unusual event, it initiates a secondary authentication unit. This is again a sensor that detects the traces of the event. If the second sensor detects the same, it authenticates the event and switches ON the wireless camera. This system has multiple advantages like reduced power consumption, improved event detection accuracy, longer life span, and enhanced information clarity. D. Arjun et al (Arjun and Indukala, 2017) describes in his paper the current Wireless Sensor Network (WSN) techniques related to border surveillance and intruder detection. Harish Bhaskar (Bhaskar, 2012) proposed integration of simultaneous detection, following, and face-acknowledgment based identification of human targets from a static camera is proposed. The precision, effectiveness, and heartiness of the proposed work are assessed and illustrated over different standard datasets over a wide scope of scenarios utilizing appropriate performance metrics. Jun He et al (He and Fallahi, 2011) demonstrate an ad-hoc WSN system for border surveillance. The network consists of heterogeneously autonomous sensor nodes that distributively cooperate with each other to enable a smart border in remote areas. This work also presents algorithms designed to maximize the operating lifetime of the deployed sensor network.

3. BORDER AND SENSITIVE SITE SURVEILLANCE

To meet the requirements of a border control policy that meets the needs of territorial security and enhanced deterrence against potential irregular migrants and to strengthen internal security and the fight against terrorism and organized crime and other illegal activities such as trafficking, illicit trafficking of migrants at the same time to facilitate the legitimate movement of persons and goods, while maintaining border security and protecting the privacy of individuals, we had the idea to model a system that will make it possible to better control movements at borders and to better manage migrations, which autonomously detects unwanted individuals through gestures and not their facial recognition while protecting the privacy of individuals. In our contribution, we assume that all the people that the drones equipped with cameras capture in the filmed area can be classified into two classes: gestures of border soldiers and gesture of terrorists and non-soldier people, our system is characterized by the following properties:

- The ability to protect the privacy of individuals to the general public. A person who does not have access can only see the private information (face and body) of the people. Initially, all the people filmed are considered "in good faith" and they are masked. Once a person is detected as unwanted individuals then that person's private information is automatically unmasked.
- The original video can be retrieved by persons with authorized access who are usually the authorities with special security clearances. For example, border guards can have access to data and with a private key can retrieve original videos to solve an investigation.
- Detect unwanted individuals through their gestures even if they hide their faces or change their look by disguising themselves.
- The automatization of the detection of the different situations of risk and to help the border guards to make decisions appropriated to ameliorate the control of the border.

In the literature, the systems proposed in section 2 have a flaw is that they do not ensure the privacy of all people since they allow hidden only privacy information for certain authorized persons and known in advance. These systems cannot be used in public places where they can be placed only in restricted and refined areas. The objective of our offered system is to assure private life not only for some allowed person but for all persons. For it, we used human gestures (instead of facial recognition) to discern if a person is undesirable or not to conceal all persons. The general architecture of the proposed system is shown in the following figure.

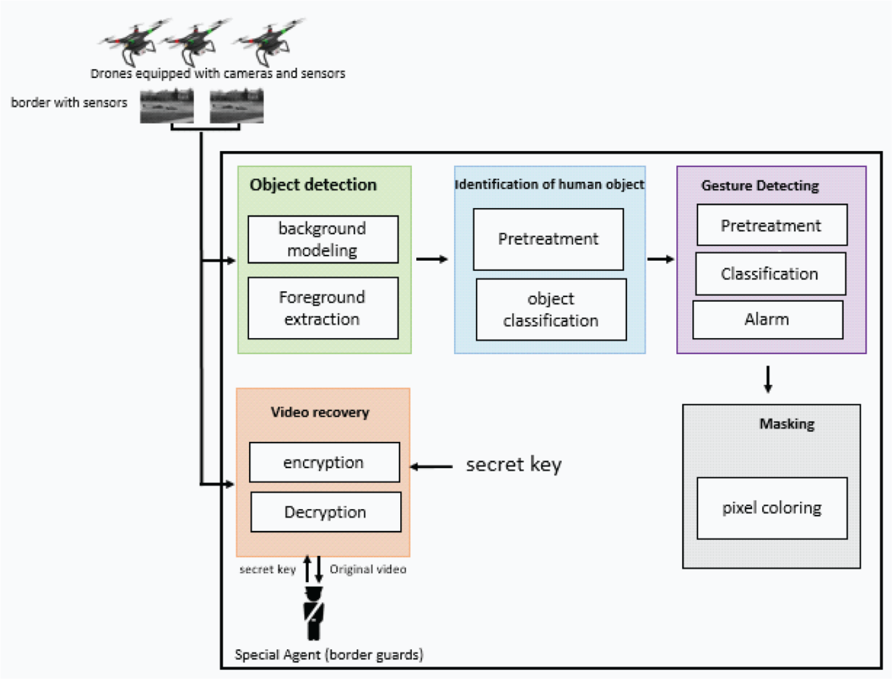
As shown in the figure above, the cameras integrated or added to the drone represent the main elements of each surveillance system. They are used to cover the entire area of interest and provide a global and detailed view to track objects and extract additional information, for example, the class of an object (person, car, truck).

3.1 Object Detection

This module consists of identifying objects in an image. This requires a segmentation step to partition a digital image into several groups (pixel set). Each group is supposed to correspond to an object in the image. In a video surveillance scenario, the goal is to separate the areas of the scene that belongs to the background from the regions belonging to the foreground namely the moving objects. For this step, a background subtraction algorithm is used that can provide real-time results to automatically generate the silhouette of human actions presented in video image sequences, where the data from each camera is processed by the following two steps:

- **Background modeling:** This step is implemented by creating a model that represents the regions of the scene that remain constant over time. For this, we propose the use of the Gaussian statistical

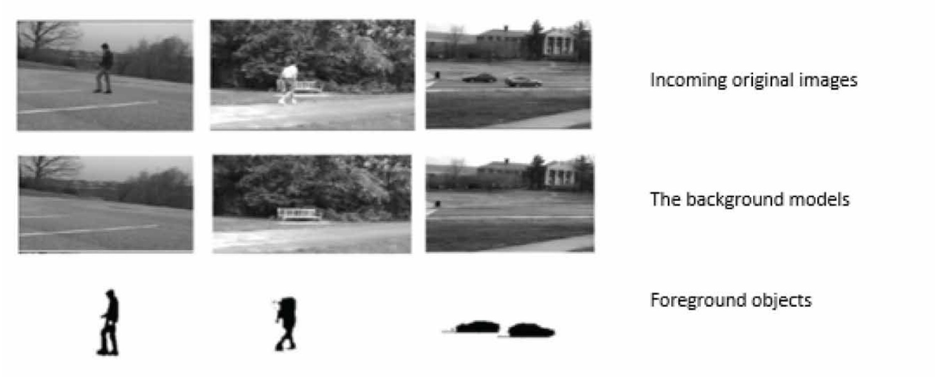
Figure 1. General architecture of the system for Surveillance of Borders and sensitive sites based on gestures



model since it gives precise results in real-time compared to the other background subtraction methods (Hu and Tan, 2004).

- **Extracting objects from the foreground:** Once the background pattern is calculated, the foreground objects are detected by calculating the difference between the original image and the background pattern as shown in the following figure. The output of this operation is a binary mask called foreground image containing objects that move in the filmed area.

Figure 2. An example of background subtraction and extraction silhouettes of foreground objects moving in three different images



3.2 Identification of Human Objects

This module aims to classify interesting objects in the field of vision of the camera (s) since in our work we are interested only by the movement of humans. For this reason, it is necessary to label each moving object to distinguish humans from other objects. The entry of this step is the silhouettes of moving objects extract from the images (video sequence) by the previous step. In this case, we are faced with a supervised classification problem since the purpose is to classify each moving object in one of two classes (person and other objects) using pre-classified images by an expert as learning data. For the realization of this stage, we can to complete this step we can follow a two-step process:

- **Binary image preprocessing:** This step detailed in section 3.3.1, is to transform each bit mask (foreground object image) to a vector.
- **Object classification:** We used the k-nearest neighbors (KPPV) algorithm, which requires the presence of a learning base consisting of images pre-classified by an expert (each image is a binary mask containing the silhouette of an object). Afterwards, a distance is calculated between each new image to be classified with each frame of the learning base.

3.3 Detection of Undesirable Persons

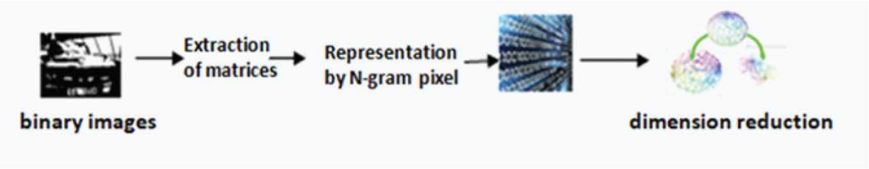
Once the silhouette of the object in an image is labeled as a person then we analyze this object in order to detect whether it is an undesirable persons or not through its gesture present by the silhouette. The classification of human gestures is a problem of binary classification (undesirable human gesture and border soldier's gesture). For the realization of this module the algorithms of supervised classification can be used where we applied the classifier of the artificial cockroaches detailed in section 3.3.2 after a stage of vectorization of each gesture of a human realized by the pretreatment process (see section 3.3.1). On the other hand if the object detected is not a human then nothing will be reported.

3.3.1 Preprocessing of Binary Images

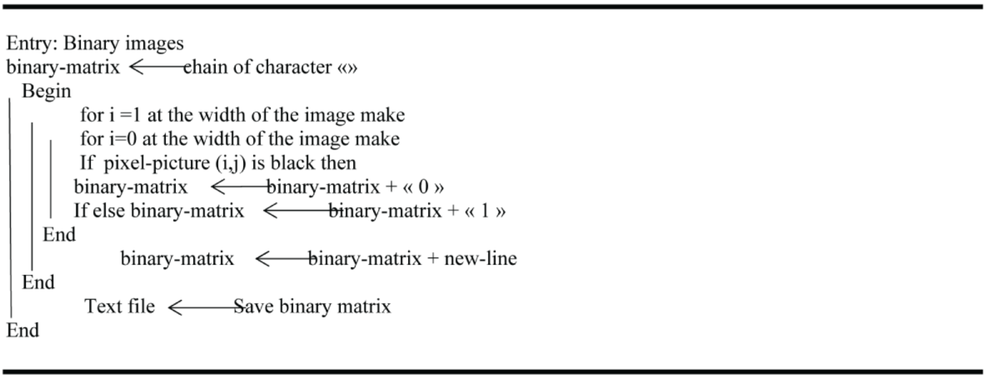
When the data entered into our software are binary images then the pre-processing steps are as follows:

- **Extraction of Matrices:** Pixels in our pictures are in color RBG, therefore for the extraction of the matrix we compare the stocks RBG of every pixel with the stocks RBG of color black (R = 255, G = 255, B = 255) and white (R = 0, G = 0, B = 0). If it am black we shall replace RGB with zero, otherwise we shall replace it with one. Finally, we shall stock every matrix in a text file. Pseudo code 1 encodes according to sums up this stage.
- **Representation by N-gram pixel:** We had the idea of representing N-Gramme pixels, trying to mimic the representation N-gram characters. Each binary matrix of an image (built from the previous phase) is considered a text and each pixel is taken as a character and we follow the same instructions of the N-gram character technique. The basic principle is that two images are similar if they carry the same elements (N-gram pixels). This step ensures the transition of each image to a set of small units called N-Gram pixels.

Figure 3. The preprocessing steps for binary images (black and white)



Pseudo code 1. Binary Matrix Extraction



```
Entry: Binary images
binary-matrix ⟵ chain of character «»
  Begin
        for i =1 at the width of the image make
        for i=0 at the width of the image make
        If  pixel-picture (i,j) is black then
        binary-matrix   ⟵ binary-matrix + « 0 »
        If else binary-matrix   ⟵ binary-matrix + « 1 »
    End
            binary-matrix   ⟵ binary-matrix + new-line
  End
        Text file ⟵ Save binary matrix
End
```

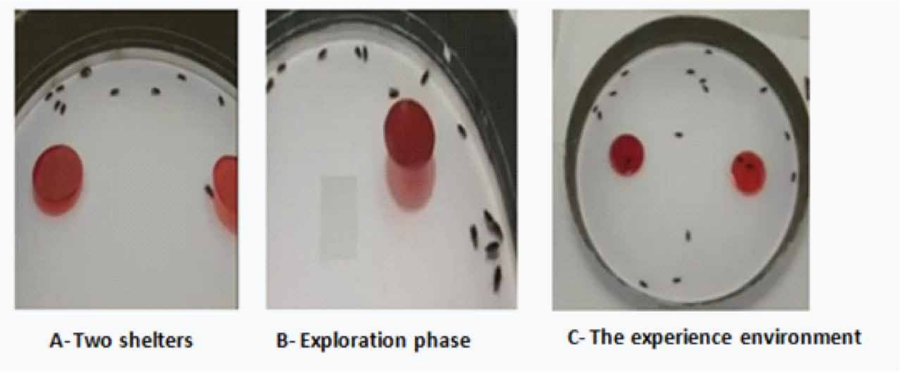
3.3.2 Grouping Cockroaches Classifier (GCC)

- **The Origin of the Algorithm:** We used the studies carried out by Bell on the social life and behavior of cockroaches in (Bell and Roth, 2007).
- **The Inspiration Source:** GCC is inspired by the natural behavior of cockroaches and the phenomenon of seeking the most attractive and secure place (shelter) for hiding. We can identify different types of cockroaches in our work, we are interested by the cockroaches that live in apartments, which are fertile and they are never isolated. This phenomenon is well detailed in an experiment conducted by French biologists when they met a group of cockroaches in a basin where there's light everywhere, and they built two artificial shelters (shelter is a place with less brightness as shown in the figure) using two red circles because cockroaches do not observe the color red as shown in the following figure (Figures 4 and 5).

The groping of cockroaches under the same place (Bell and Roth, 2007).

From previous experience it was observed that cockroaches have a choice of two shelters to hide where they always choose the most secure shelter. A biological model explaining this phenomenon is presented by the following:

Figure 4. Description of the experience



A-Two shelters

B-Exploration phase

C-The experience environment

Figure 5. The groping of cockroaches under the same place (Bell and Roth, 2007)

- **Random Displacement of Cockroaches:** Initially cockroaches will move randomly in all directions (exploration phase) as demonstrated in Figure 4.b. When a cockroach finds an attractive shelter, it hides and sends pheromones as smell to its congeners. The movement of cockroaches is guided by a set of displacement rules:
  - **The Darkness Shelters:** Cockroaches are attracted by the darkest places like corners and shelters with less brightness. The degree of darkness plays a very important role for the quality security of each shelter.
  - **The Congener's Attraction:** Each cockroach seeks shelter where there are more of its congeners (cockroaches from the same colony) to hide it.
  - **The Security Quality:** Cockroaches positioned in the middle of the shelter have a higher safety compared with cockroaches positioned at the border of the shelter.
- **General Processes:** In the supervised classification problem the data set is divided into two bases (learning basis and test basis). Each new instance (cockroach) well be classified (hidden) in a class (shelter) using a security function that is based on the attractiveness of each class (calculated using the aggregation operators (shelter darkness, congeners attraction and the quality of security), and the displacement probability (calculated using the naive Bayes algorithm). the general process of the GCC is illustrated in the next figure.

The general architecture of Grouping Cockroaches Classifier (GCC) is illustrated in Figure 6 and each stage of its operation is described below.

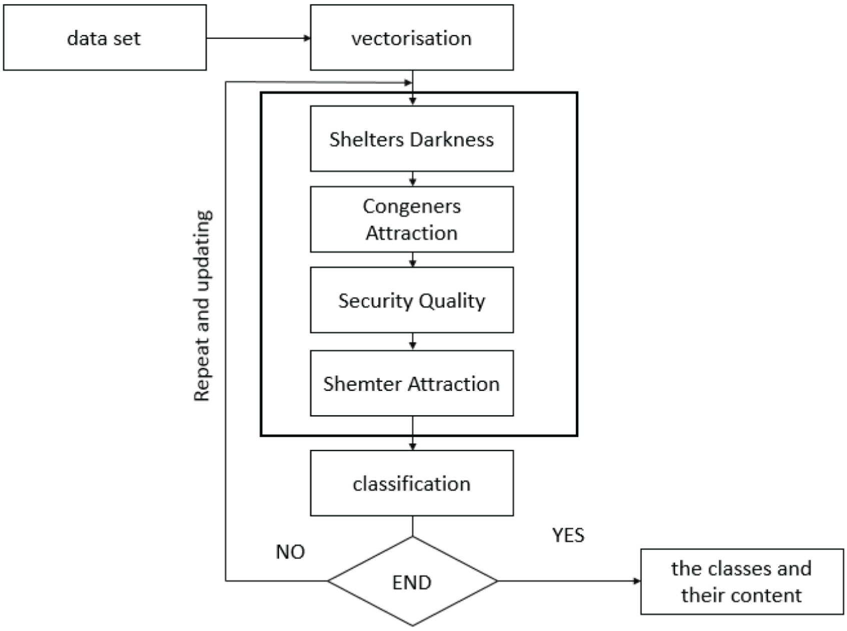
The vectorization of the data carried out according to the process detailed in section 3.3.1.

1. **The Darkness Shelters:** The Darkness Shelters calculates the rate of darkness in each shelter that represents the number of instances belonging to each class (shelter) relater à relative to the total number of instances in all classes. Initially, the cockroaches of the learning base are hidden in each corresponding shelter (we know the instances classes of the learning basis):

$$\text{OA}\ (S_i) = \frac{CS_i}{\#CL} \tag{1}$$

  - **CSi:** The number of instances belonging to the class S_i (the number of cockroaches in the shelter).
  - **#CL:** The total number of instances in all classes (the total number of cockroaches in the shelter).
  - **OA ($\mathbf{S_i}$):** The darkness rate of the shelter S_i.

Figure 6. The general functioning of Grouping Cockroaches Classifier (GCC)



2. **The Congeners Attraction (CA):** As shown in equation III.2, The CA is defined by a parameter K fixed in advance, and for each new instance classifying Cn, we randomly select k instances (designated as k congeners for the cockroach Ci in the shelter Si) of each class. Then, the total number of instances belonging to this class divides the sum of the distances between this instance and its K congeners:

$$\text{CA}\ (C_n\ ,\ S_i) = \frac{\sum_{K=1}^{K} distance\left(C_n, C_K S_i\right)}{\# CS_i} \tag{2}$$

- ◦ **CKSi :** The Kem nearest neighbour instance cn in the class Si.
- ◦ **Distance$\left(\mathbf{Cn, CK\ Si}\right)$:** The distance between the instances to be classified Cn and its k nearest neighbors in the class Si.
- ◦ **K :** The number of selected instances.
- ◦ **CSI :** The total number of instances in the classes S.

3. **The Security Quality:** A cockroach must be in good condition to stay in a shelter and it has a maximum quality of security when it is close to the middle of the shelter. The security quality of the instance Cn in a class Si is calculated through equation III.3:

$$\text{QS}\ (C_n\ ,\ S_i) = distance\left(C_n, BS_i\right) \tag{3}$$

- ◦ **BS$_\mathbf{i}$:** The centroid of the class S_i.

4. **Shelter Attraction:** We use the results of the previous aggregation operators to calculate the attraction of each class for each instance as follows:

$$\text{SA}\ (C_n\ ,\ S_i) = \frac{\alpha * OA\left(S_i\right)}{\beta * CA\left(C_n, S_i\right) + \lambda * QS\left(C_n, S_i\right)} \tag{4}$$

   - **α, ß et ʎ:** The Adjustment coefficients to adjust the impact of each operator in calculating the attractiveness of each class.

5. **Probability of displacement:** For this, to calculate this probability we used the naive Bayes algorithm. Bayes' theorem provides a way to assign each instance a probability for each possible class. He assumed that the effect of the value of a predictor (xn) on a given class (Si) is independent of the values of other predictors. the probability of each instance to be classified in a class Si is calculated by the next equation:

$$P\left(Si\ /\ Cn\right) = \text{P}(x_1,\ S_i)\text{*}\ \text{P}(x_2,\ S_i)\text{*}\ldots\text{*P}(S_i) \tag{5}$$

   - **P (S_i l C_n):** The posterior probability is the probability that the instance Cn is classified in the class (Si).
   - **P (S_i):** Is the prior probability of the class Si.
   - **P (x l Si):** Is the probability that component x generates the class Si.

6. **The security function:** The cockroach always belongs to the most attractive shelter where it is more likely to reach it (each new instance will be classified in the most attractive class where it has more probability). For this, we used the security function f (Ci, Si) which allows us to find the most appropriate class for each instance (the most secure Si shelter for each cockroach Cn). The final decision concerning the class of each instance is done following the value of the security function:

$$\text{f}(C_n\ ,\ S_i) = SA\left(Cn, Si\right) + P\left(Si\ /\ Cn\right) \tag{6}$$

   - $\mathbf{SA\left(Ci, Si\right)}$**:** The attraction of the class Si for the instance Cn.
   - $\mathbf{P\left(Ci, Si\right)}$**:** The probability of the cockroach Ci to be classified in the class Si.

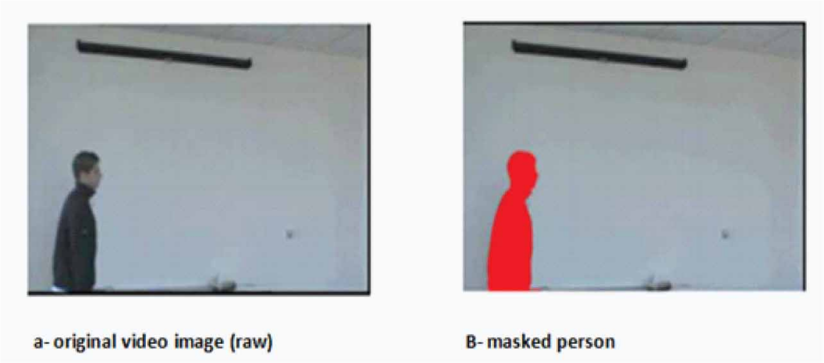
   Each instance is classified in the shelter that has the highest value of the safety function.

7. **Update:** After each iteration, we update the values of the aggregation rules and the probability of displacement for each instance, when a cockroach does not feel safe (instance is miss-classified), then it will look for another more secure shelter (we reclassify this instance again). The process is repeated until a stopping criterion.
8. **Stop criterion:** The stopping criterion GCC is the number of iterations fixed in advance, or if the number of instances in each class remains the same for the iteration i and iteration i + 1.

3.4 Masking Normal People

Once a person's gesture in the binary mask is detected as border soldiers then that person's face and body will be automatically hidden following the pixel coloring technique (Yang, 2003) as shown in

Figure 7. Example of masking of a person using the pixel coloring approach that hides privacy details such as the face and body


a- original video image (raw)

B- masked person

the next figure in order to hide his privacy information. On the other hand, if the person is detected as undesirable persons then his or her privacy information will not be hidden.

3.5 Alarm

Our border surveillance system should be able to respond to specific events. Once a person is detected as unwanted then an alarm will be triggered. The goal is to tell the screening officers or users of this system that they are in a situation with an abnormal event and that you have to intervene by following in that person's footsteps or trying to arrest that person.

3.6 Original Video Recovery

In the event that people detect by our system as a border soldiers to whom we have hidden their privacy information (face and body) have been involved in some evil or criminal behaviors, our system has the ability to provide original surveillance images when necessary. In this sense, our system can provide access to special authorities who have a secret key, such as border guards, who can observe all the information that has arrived in the guarded space. The simplest solution to this problem is to store a copy of the original encrypted surveillance video separately.

4. EXPERIMENTATION AND RESULTS

4.1 Experiments

Given that our system is primarily based on detecting people who cross the border illegally even if they hide their faces based on human gestures instead of facial recognition, we will only present the results experimental purposes for this part of the system only. Before we begin our experimental protocol, we must first determine the baseline data set used.

4.1.1 The MuHaivi Dataset

1. **Video Clips:** A significant body of human action video data has been collected using 8 Schwan CCTV cameras in a site with challenging lighting conditions. The cameras are located at 4 sides and 4 corners of a rectangular platform (Figure 8 and Table 1). These cameras are not automatically synchronized, but the video segments for each action/actor combination have been manually synchronized. There are 17 human action classes (Cj: C1, C2, ..., C17) as listed in Table 2 performed by 14 actors (Ak: A1, A2, .., A14). The video sequences contain a number

Figure 8. View of the configuration of eight cameras used to capture actions in the blue action area (marked with white bands on the floor of the stage) (Singh and Velastin, 2010)

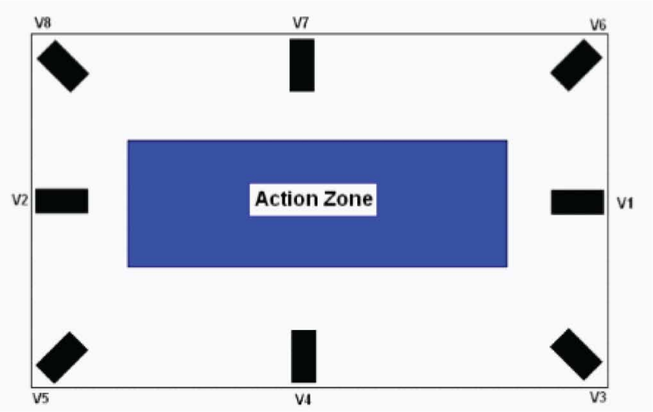
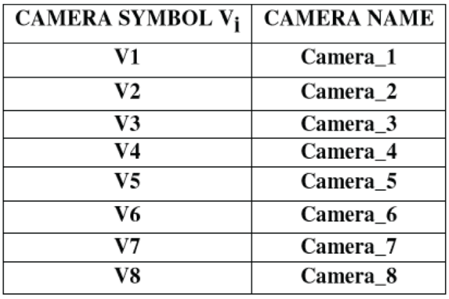


Table 1. The names of the camera views used in the data record and the corresponding symbols used in Figure 8 (Singh and Velastin, 2010)



CAMERA SYMBOL V_i	CAMERA NAME
V1	Camera_1
V2	Camera_2
V3	Camera_3
V4	Camera_4
V5	Camera_5
V6	Camera_6
V7	Camera_7
V8	Camera_8

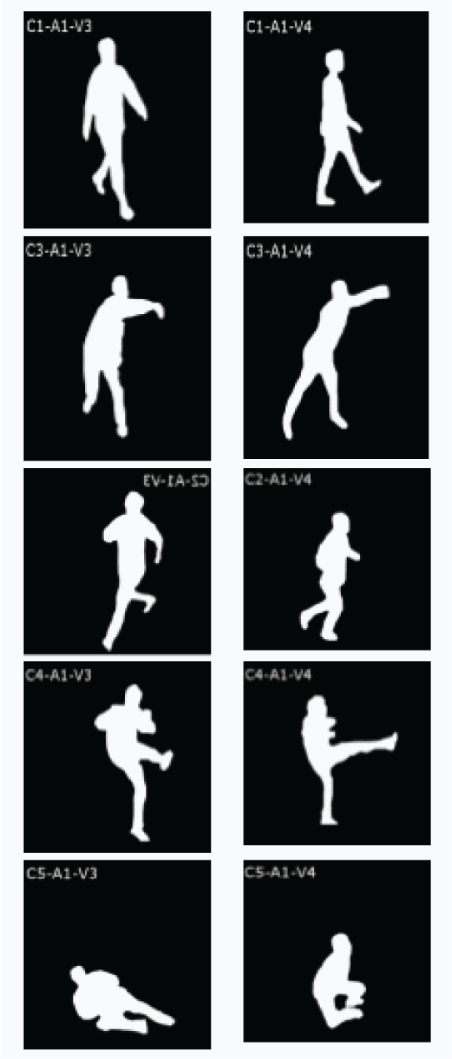
of image frames before the action takes place so as to allow background estimation algorithms sufficient time to model the background, if necessary (Singh and Velastin, 2010).

2. **Silhouettes Manually Annotated:** The dataset provides a sub-set of data that has been (painstakingly) manually annotated. This of course reduces the size of the data available for "pure" action recognition. A detailed performance evaluation of state-of-the-art object detection algorithms using this small sub-set of data is currently underway with the view to select a robust method to compute these silhouettes automatically.

This subset of manually annotated data consists of actions C1... C5, actors A1 and A4 and cameras V3 and V4, therefore a total of 5 x 2 x 2=20 actions. Samples of the manually obtained silhouettes are shown in Figure 5.3. Although actions C1... C5 are relatively elemental from a human point of view, they can still be decomposed further into primitive actions. (Singh and Velastin, 2010).

They grouped the images of the actions as a class of images of the gestures of terrorists and non-soldier people and on the other hand images of the actions of border soldiers gestures. The modified MUHAVI dataset is defined in Table 3. Each gesture-based unwanted person detection algorithm has as input learning data pre-classified by an expert (binary masks for gestures of unwanted persons and

Figure 9. Views of all 8 cameras showing examples of measurements and actors sample camera symbols as in Figure 8

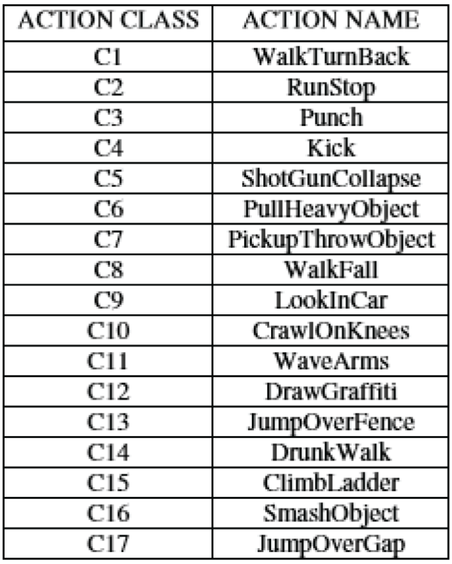


other for the actions of border soldiers). The following table represents the redistricting of the data used to conduct our tests (learning and test data).

4.2 Results and Analysis

To test the Border surveillance module only, we used the Grouping Cockroaches Classifier (GCC) with iteration number 1 and weights of the aggregation rules (α=1, ß=1 and ʎ=1) as well as K=1. For this we applied the GCC to the muhaivi dataset detailed previously since it consists of a set of silhouettes of humans annotated manually which does not require testing the object detection and identification modules. Human beings. For validation of the results obtained, we used supervised measurements with the class of terrorists and non-soldier people as a positive class in the contingency matrix. We conducted different tests in order to analyze the performance of the GCC by studying the influence of each parameter.

Table 2. The action class names used in the data record and the corresponding symnoles used in Figure 9 (Singh and Velastin, 2010)



ACTION CLASS	ACTION NAME
C1	WalkTurnBack
C2	RunStop
C3	Punch
C4	Kick
C5	ShotGunCollapse
C6	PullHeavyObject
C7	PickupThrowObject
C8	WalkFall
C9	LookInCar
C10	CrawlOnKnees
C11	WaveArms
C12	DrawGraffiti
C13	JumpOverFence
C14	DrunkWalk
C15	ClimbLadder
C16	SmashObject
C17	JumpOverGap

Figure 10. Examples of manually annotated silhouettes (Singh and Velastin, 2010)

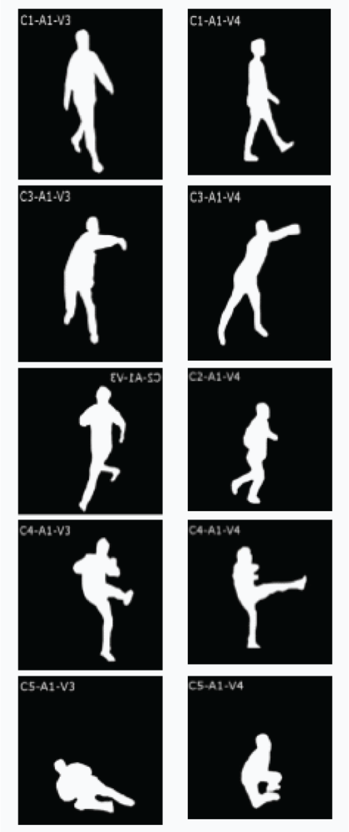


Table 3. Muhaivi dataset decomposition

	Number of learning images	Number of test images	Total
Gestures of terrorists and non-soldier	200	314	514
Gestures of border soldiers	100	326	426

4.2.1 The Influence of Image Representation and Distance Measurement

Before applying the GCC a process of vectoring the images is necessary. We have varied the value of the N parameter used by the N-grams pixel representation method in the pre-processing phase and each time we set a distance measurement to assess the quality of each output. The results are detailed in the following tables.

In our contribution, the main idea is that two images are identical if the number of occurrences of each N-pixel in these two images are the same. After observing the results in Tables 4, 5 and 6 we noticed that:

- The Manhattan distance measurement gives the best results compared to the cosine and Euclidean distance validated by an f-measure=0.8804 and entropy=0.0897 (blue cases in Table 6) because our goal is to find the exact difference between the vector components. In other words, two gestures are different if the occurrence values of their vector components are distant from each other. The distance between Euclidean and Manhattan give good results in relation to the cosine distance because we are interested in the magnitude of the image and not only by the relative frequencies of the N-pixels in the images.
- The recall is always less than the accuracy given that the majority of cases are classified as a border soldiers gesture validated by the contingency matrix with FN=45 and VN=298 (the green cases of Table 6) because on the one hand malicious or criminal persons always try to hide their appearances and be as normal as possible and on the other hand the learning data we used does not aggregate all the gestures of terrorists and non-soldier people that may exist. We may also have a conflict in detection between border soldiers and undesirables person.

Table 4. Undesirables person detection results based on human gestures using Euclidian distance and variation of the N parameter for N-grams pixel representation

		Evaluation Measures							
		Recall	Precision	F-Measure	Entropy	Success Rate	Contingency Matrix		
								U	N
							U	TP	FP
							N	FN	VN
N-Gram Pixel	2-gram	0.7229	0.8376	0.776	0.1484	79.53	227		44
							87		282
	3-gram	0.7675	0.8743	0.8124	0.1174	83.125	241		35
							73		291
	4-gram	0.8184	0.8862	0.8506	0.107	85.937	257		33
							57		293
	5-gram	0.8248	0.8961	0.859	0.0983	86.71	259		30
							55		296

Table 5. The detection results of undesirables people based on human gestures using cosinus distance and variation of the parameter N for the N-grams pixel representation

		Evaluation Measures							
		Recall	Precision	F-Measure	Entropy	Success Rate	Contingency Matrix		
								U	N
							U	VP	FP
							N	FN	VN
N-Gram Pixel	2-gram	0.694	0.767	0.7289	0.2034	74.68	218		66
							96		260
	3-gram	0.7006	0.7885	0.745	0.1873	76.093	220		59
							94		267
	4-gram	0.707	0.8014	0.7511	0.1774	77.03	222		55
							92		271
	5-gram	0.7197	0.8071	0.7638	0.1729	77.81	226		54
							88		272

Table 6. The detection results of illegal migrants based on human gestures using the Manhattan distance and variation of the parameter N for the representation of images

		Evaluation Measures							
		Recall	Precision	F-Measure	Entropy	Success Rate	Contingency Matrix		
								U	N
							U	VP	FP
							N	FN	VN
N-Gram Pixel	2-gram	0.799	0.8655	0.8308	0.125	84.062	251		39
							63		287
	3-gram	0.8216	0.8896	0.8542	0.104	86.25	258		32
							56		294
	4-gram	0.8566	0.9057	0.8804	0.0897	88.59	269		28
							45		298
	5-gram	0.8503	0.89	0.8696	0.1037	87.5	267		33
							47		293

- Every time we increase the value of the N parameter, the results improve because the vectors will be made up of more components, making it possible to better differentiate between 2 images of any kind. For example the 2-gram pixels can generate only 4 components (00, 01, 10, and 11), the 3-gram pixels generates 8 components (001, 100, 010, 110, 111, 000,001, 011) and so on.
- In terms of success rates even though we will get a percentage of 88% but this is not enough as part of our goal since it means that it has a lot of false alarm report (border soldiers detect as undesirable people) and the private information of innocent people will be revealed to the normal public.
- In terms of entropy, the results are clearly performing as the accuracy is elevated because we did not use the normalization of images, which allowed getting less loss of information.

4.2.2 Comparative Study

- **Statistical Comparison:** To give more reference to our results obtained, we have put in confrontation the best performance of our Classifier of Grouping Cockroaches (GCC) in the face of the problem of detection of illegal migrants based on gestures against the results of other algorithms that exist in the literature such as classical learning algorithms like the nearest Nearby K (KPPV) with K=1 and cosine distance and C4.5 decision trees that have been applied using the WEKA API that provides tools and libraries ready to be used directly. The results of this comparison are presented in Table 7.

It should be noted in the table that the maximum value in the f-measure=0.8804 is obtained with the classifier of artificial cockroaches (blue cases) because it is based on different rule and property as (attraction of congeners, darkness of the shelter, the quality of safety, and the likelihood of travel). We also found that the convergence of this classifier takes a lot of time given the number of calculations and its complexity which requires several tests and comparisons.

KPPV classifiers give almost similar results to GCC (the yellow cases in the table) because they are based on a direct and naïve operation using a distance measurement. On the other hand the bad results are obtained by the decision tree C4.5 method, because we are faced with binary images and the C4.5 is based on the gain of the ration and cannot identify the optimal root (prove in the literature).

- **Comparison in Terms of Services:** What are the reasons for a good or poor performance of a video surveillance system for undesirable detection tasks? Table 7 compares our system with four other systems that exist in the literature (Drone-Aided Border Surveillance with an Electrification Line Battery Charging System (Kim and Lim, 2018), WSN-based Border Surveillance Systems(Arfaoui and Boudriga, 2017), An efficient WSN based solution for border surveillance (Laouira, Abdelli, 2019), Internet of Things based High Security Border Surveillance Strategy (Karthick and Prabaharan, 2019); Wireless IoT-Based Intrusion Detection Using LIDAR in the Context of Intelligent Border Surveillance System (Segireddy and Koneru, 2020)) from several angles such as: The preservation of the privacy of all undesirable persons:
    - Automatic detection.
    - The ability to detect undesirable people who hide their faces.
    - The ability to retrieve original videos.
    - Detect and unmask undesirable individuals automatically.
    - Location of use.

From the previous table, we note that our proposed system (the blue cases in Table 8) can be used in any location as it clearly meets all the requirements of a modern security policy by providing all services to ensure the safety of citizens and the government with the preservation of privacy. Unlike

Table 7. Comparative study in terms of the quality of results of different classifiers for the detection of unwanted persons based on gestures

		Evaluation Measures				
		Recall	**Precision**	**F-Measure**	**Entropy**	**Success Rate**
Classifiers	**K nearest neighbors**	0.8429	0.8681	0.853	0.1227	84
	Decision tree C4.5	0.6497	0.7329	0.695	0.2306	67.2
	Grouping Cockroaches Classifier	0.8503	0.89	0.8696	0.1037	87.5

Table 8. Comparison in terms of services between our system and 4 other systems which exist in literature

	Our proposed system	Drone-Aided Border Surveillance with an Electrification Line Battery Charging System (Kim and Lim, 2018)	WSN-based Border Surveillance Systems (Arfaoui and Boudriga, 2017)	An efficient WSN based solution for border surveillance (Laouira, Abdelli, 2019)	Internet of Things based High Security Border Surveillance Strategy (Karthick and Prabaharan, 2019)	Wireless IoT-Based Intrusion Detection Using LIDAR in the Context of Intelligent Border Surveillance System (Segireddy and Koneru, 2020)
Privacy Preservation	Yes	No	No	No	No	No
Automatic detection with alarm	Yes	NO	No	Yes	Yes	Yes
Detection of undesirable people who hide their faces	Yes	No	No	No	No	Yes
Revelation of original videos for authorized persons	Yes	No	No	No	No	Yes
Unmask undesirable people automatically	Yes	NO	Yes	No	No	No
Place of use	international border and sensitive site	international border between countries	international border between countries	international border between countries	international border	international border

other systems that exist in the literature where each of them has shortcomings especially in terms of privacy as well as their inability to detect people who hide their faces.

4.3 Decisions

1. Every time we increase the N value of the N-gram pixel representation the results improve.
2. The adaptation of the N-gram technique for the representation of binary images was a very interesting experience since it does not require the normalization of images and it is tolerant to the problems of incomplete images.
3. The ideal configuration of the Grouping Cockroaches Classifier (GCC) is:
    a. 4-gram pixel as a method of representation.
    b. Manhattan as a measure of distance.
4. The GCC gives better results than classifiers like the KPPV and C4.5 decision tree.
5. The GCC takes a lot of time to run compared to other conventional learning algorithms.

Our private detection system for undesirable's persons provides many advantages in terms of quality of services compared to other video surveillance systems that exist in the literature.

5. CONCLUSION AND FUTURE WORK

We introduced a méta-heuristic news of tattletale for the surveillance of borders through videos captured by one of the drones via sensors; this algorithm is inspired of work of researcher's biologists who discovered the links of communication between the Cockroaches and their behavior. Acquired results are satisfactory and prove that algorithm is able of guaranteeing surveillance of borders. It gives better results in comparison with other algorithms existing in literature (k-means, tree of decision, C4.5), Validated by the measurements of valuation (recall, precision, Fr - Measure, entropy, rate of success, rate of error) We studied the impact of every parameter for the quality of performance of every algorithm to identify ideal. Finally, we can conclude that our contentment is full because targets fixed at the beginning were reached. For our future work, we will can extended this system for use on a larger scale then the system can be equipped with the mobile-based applications. Since IoT provides a global coverage, the data that is generated from the system can be accessed anywhere over the earth. Besides, we would like to propose to use an architecture based on deep learning in future work in order to improve our system.

ACKNOWLEDGMENT

Authors would like to acknowledge the DGRSDT (Directorate General of Scientific Research and Technological Development under the authority of the Algerian Ministry of Scientific Research) for its support to this work and to the GeCoDe Laboratory.

REFERENCES

Al Abkal, S., Talas, R. H. A., Shaw, S., & Ellis, T. (2020). The application of unmanned aerial vehicles in managing port and border security in the US and Kuwait: Reflections on best practice for the UK. *International Journal of Maritime Crime and Security*, *1*(1).

Arfaoui, I., Boudriga, N., Trimeche, K., & Abdallah, W. (2017). WSN-based Border Surveillance Systems Using Estimated Known Crossing Paths. *MoMM2017.*

Arjun, D., Indukala, P. K., & Menon, K. U. (2017, April). Border surveillance and intruder detection using wireless sensor networks: A brief survey. In *2017 International Conference on Communication and Signal Processing (ICCSP)* (pp. 1125-1130). IEEE.

Bell, W. J., Roth, L. M., & Nalepa, C. A. (2007). *Cockroaches: ecology, behavior, and natural history*. JHU Press.

Bhadwal, N., Madaan, V., Agrawal, P., Shukla, A., & Kakran, A. (2019). Smart Border Surveillance System using Wireless Sensor Network and Computer Vision. *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, 183-190.

Bhaskar, H. (2012, September). Integrated human target detection, identification and tracking for surveillance applications. In *2012 6th IEEE International Conference Intelligent Systems* (pp. 467-475). IEEE.

Goyal, A., Anandamurthy, S. B., Dash, P., Acharya, S., Bathla, D., Hicks, D., & Ranjan, P. (2020). Automatic Border Surveillance Using Machine Learning in Remote Video Surveillance Systems. In *Emerging Trends in Electrical, Communications, and Information Technologies* (pp. 751–760). Springer.

He, J., Fallahi, M., Norwood, R. A., & Peyghambarian, N. (2011, June). Smart border: ad-hoc wireless sensor networks for border surveillance. In Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense X (Vol. 8019, p. 80190Z). International Society for Optics and Photonics.

Hu, W., Tan, T., Wang, L., & Maybank, S. (2004). A survey on visual surveillance of object motion and behaviors. *IEEE Transactions on Systems, Man and Cybernetics. Part C, Applications and Reviews*, *34*(3), 334–352.

Karthick, R., Prabaharan, A. M., & Selvaprasanth, P. (2019). Internet of things based high security border surveillance strategy. *Asian Journal of Applied Science and Technology*, *3*, 94–100.

Kim, S. J., & Lim, G. J. (2018). Drone-aided border surveillance with an electrification line battery charging system. *Journal of Intelligent & Robotic Systems*, *92*(3-4), 657–670.

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: A review. *Journal of Big Data*, *6*(1), 111. doi:10.1186/s40537-019-0268-2

Laouira, M. L., Abdelli, A., Othman, J. B., & Kim, H. (2019). An efficient WSN based solution for border surveillance. IEEE Transactions on Sustainable Computing.

Segireddy, S., & Koneru, S. V. (2020). Wireless IoT-Based Intrusion Detection Using LIDAR in the Context of Intelligent Border Surveillance System. In *Smart Intelligent Computing and Applications* (pp. 455–463). Springer.

Singh, S., Velastin, S. A., & Ragheb, H. (2010, August). Muhavi: A multicamera human action video dataset for the evaluation of action recognition methods. In *2010 7th IEEE International Conference on Advanced Video and Signal Based Surveillance* (pp. 48-55). IEEE.

Sood, P., Sharma, H., & Sehra, S. K. (2019). A Survey of Different Methods in Border Security and Surveillance. *International Journal on Computer Science and Engineering*, *7*(10), 217–228.

Yang, R. (2003). *View-dependent Pixel Coloring: A Physically-based Approach for 2D View Synthesis* (Doctoral dissertation). University of North Carolina at Chapel Hill.

Abdelmalek Amine received an engineering degree in Computer Science, a Magister diploma in Computational Science and PhD from Djillali Liabes University in collaboration with Joseph Fourier University of Grenoble. His research interests include IoT, bigdata, data mining, text mining, ontology, classification, clustering, neural networks, and biomimetic optimization methods. He participates in the program committees of several international conferences and on the editorial boards of international journals. Prof. Amine is the head of GeCoDe-knowledge management and complex data-laboratory at UTM University of Saida, Algeria; he also collaborates with the "knowledge base and database" team of TIMC laboratory at Joseph Fourier University of Grenoble.

Reda Mohamed Hamou received an engineering degree in computer Science from the Computer Science department of Djillali Liabes University of Sidi-Belabbes-Algeria and PhD (Artificial intelligence) from the same University. He has several publications in the field of BioInspired and Metaheuristic in many journals as IJAMC, IJIRR, IJAEC, IJALR, IJISP, IJIIT, JITR, IJCINI, IJOCI, IJSIR, IJSI, IJAEIS, IJDSST, IJBRA, Applied Intelligence. His research interests include Data Mining, Text Mining, Classification, Clustering, computational intelligence, neural networks, evolutionary computation and Biomimetic optimization method. He is a head of research team in GecoDe laboratory. Dr. Hamou is an associate professor in technology faculty in UTMS University of Saida-Algeria.