Preprints.org

Crime Detection and Suspect Identification System

Abdulaziz BinDarwish [*] , Salim Alhammadi , ABDULLAH SALEHI

Article

Crime Detection and Suspect Identification System

Abdelaziz BinDarwish [1,*], Salim AlHammadi [2] and Abdullah Salehi [3]

[1]   Computer Information Science, Higher Colleges of Technology, Sharjah, United Arab Emirates; rissb2@gmail.com

[2]   Computer Information Science, Higher Colleges of Technology, Sharjah, United Arab Emirates; SA_Alhammadi@outlook.com

[2]   Computer Scienc, University of Sharjah, Sharjah, United Arab Emirates; Aabdulla.salehii@gmail.com

[*]   Correspondence: mohandesosama@gmail.com

Abstract: The number of ATMs in various countries is increasing steadily and rapidly with the number of users increasing very widely. On the other hand, banks have become more interested in finding the best procedures to combat ATM crimes to ensure the safety and security of their customers and other cardholders. This has become an excellent target for some criminals or fraudsters, despite the limited amounts that can be withdrawn from these devices, given a maximum daily limit. We aim at implementing this system inside bank ATMs in order to detect objects like guns, hammers, and knives. Once the suspicious objects and actions are detected, we perform facial recognition to identify whether the suspect is a repeating offender. We use object, face, and action recognition algorithms to achieve our objective. Results showed that using our proposed algorithm is efficient in detecting threatening objects.

Keywords: crime detection; suspect identification; ATM; faces; protection

---

I. Introduction

ATMs have become one of the main sources of profit for banks that are increasingly marketing this service. In ATMs outside the bank due to the increasing number of non-customer cardholders.

We proposed a surveillance system to detect threatening objects in ATMs both inside and outdoors. This system helps banks to enhance and ensure the safety and security of their customers and other cardholders when using ATMs. Pointing to the possibility of using this system to monitor homes, jewelry stores, and other institutions through the technology of smart video [1].

This new technology will enable banks to monitor ATMs, their headquarters, their moneyboxes, offices, and buildings, in addition to many other things from one place, in addition to recording all transactions carried out in or through them, with the possibility of retrieving pictures and keeping transaction data and card number used to make the transaction [2].

This system achieves two main objectives: to deter theft and fraud and to facilitate the identification of aggressors through the recording of images and transferring them directly to the monitoring centers so that it can be recovered later in a digital way very easily. The system can also have tracking via the internet and linked to the notification service by sending text messages in the event of an emergency [3]. The new system will reduce the percentage of cyber crimes because it will enable banks to reach 99% of the perpetrators of these crimes or frauds, especially with the spread of ATMs in the halls of internal banks, hospitals, commercial complexes, and in the streets and airports [4].

Thus, these banks will be able to recover their profits. It is worth noting that billions of transactions are taking place around the world every day and are often in the form of cash withdrawals. The proposed system has several advantages that include:

- It can save live video footage and audio files for long times.
- The possibility of communication and follow-up through the Internet from anywhere in the world [5].

- Live monitoring through a Monitor or PC in one screen divided by a number of cameras.
- The ability to follow up on Mobile devices.
- Display the surveillance cameras on TV, computer, or any other screen.
- Use of surveillance cameras for night surveillance purposes
- Monitor more than one place at a time from more than one corner.
- Use of surveillance cameras at home and abroad.
- Photography and recording in extreme weather conditions.

The proposed technique examines the face, either directly through the camera or through the examination of one or more images, and measures the different facial features such as eye position, eyebrow shape, and nose length, Electronic programs in a specific database to find who matches them [6]. Thus, the police can match the image of one of the surveillance cameras that photographed a crime with the content of its database containing images taken for security purposes. The Facebook label, which is still not supported in the European Union, can automatically identify images on social media sites. This technique can also use to identify people [7,8].

For many years, facial recognition was an unreliable source of identification because computers had difficulty identifying faces, especially as people's features changed as age or weight increased, or when men released their skin [9]. They also suffered from some impurities with the optical changes or angle from which the image takes. Today, however, this technique has become remarkably accurate [10,11].

The National Institute of Standards and Technology (NIST) has confirmed that the error rate for the best facial recognition systems is only 0.8 percent. This technology may not be as good as fingerprint or fingerprint recognition systems, but it is much better than voice recognition. Compared to more precise bio-metric techniques, facial recognition has an added advantage: it does not require approval, cooperation or even knowledge of the person concerned [12,13].

A. Use of Technology

Governments are leading the list of customers of this technology, which amounts to about $ 4 billion, namely government agencies that deal with collective identification systems such as prisons, airports, vehicle licensing authorities, and, of course, police. This technique is used in Mexico to prevent fraud during voting [14].

This technique is used in consumer industries as well. The New Vision surveillance systems where developed by NEC have promised better performance to identify customers through "more pleasant and smooth entry procedures" in hotels and to identify "undesirable" people [15,16] Ontario nightclubs use this technology to avoid the problems of gamblers who were denied entry; in China, ordinary people use them to pay for their coffees or visit archaeological sites and even withdraw money from ATM machines [17,18].

B. Risks

With the proliferation of this technology, fears of its privacy and misuse have escalated. The Russian "Fined-Veiss" application, which can identify strangers by comparing their images with about 200 million profile images to social media, has been used for harassment. This use of this technology by the police has also raised people's concerns [19].

In the United States, FBI computers have access to images of half of the adults in American society, although 80% do not have a criminal record. Five police stations are working on laying cameras to identify people on the street. In Britain, the police collected about 20 million images in a searchable database using a facial recognition system. It is used in the Hill Carnival and sports competitions to identify suspects [20].

C. Deceive Surveillance Systems

Previously, it was easy to deceive facial recognition systems, where anyone could hack some identity systems by placing a picture of the user in front of the screening machine. However, it is more difficult today: In the iPhone X, for instance, its system reads the face by dropping a network of 30,000 points of infrared radiation. Simese NN can also be used for detecting face patterns [21,22] MTCNN network is used to detect faces at a distance [23,24]. The Wired magazine used a Hollywood makeup expert to make a silicon mask to trick the iPhone X camera into believing that the user was authorized to open the device, but the attempt failed.

On the other hand, there are some ways, in which the detection of face recognition systems can be confused. The wearing of a hat, scarf, or glasses can make some difference, so some designs and shapes can seriously disrupt the program.

Researchers at Carnegie Mellon University developed large color glasses that concealed the identity of those wearing them, while others used facial coatings to cover parts of the cheeks in certain colors to blind the scanner and prevent the operation of calculations necessary to identify the face. But the drawback of all these tricks to face recognition systems is that they make you the focus of everyone. "The tricks that make you invisible to computers make you a remarkable sight for people around you," says Robinson Meier of The Atlantic [25–27].

II. The Proposed Approach

The proposed approach goes through the following steps as shown in Figure 1 Step 1: Detect human behavior and weapon visibility to define if the behavior is either normal or abnormal [28,29].

Step 2: In case the behavior is normal and no weapon is visible, no action is needed. And continue the detection process.

Step 3: If the behavior is abnormal or weapons are visible, do the following steps

- Extract the key person's face
- Match their face with the suspect database
- Extract the nearest n faces
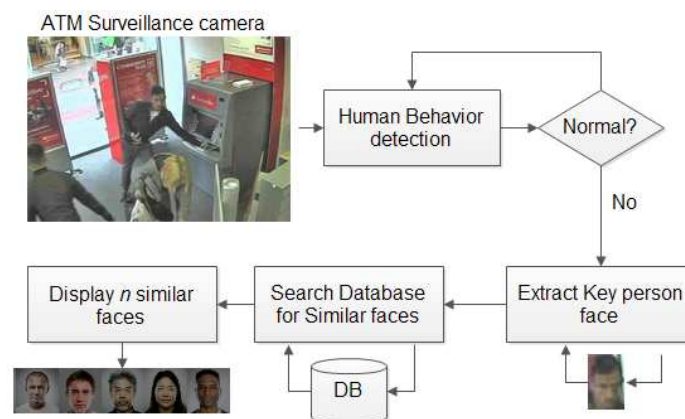- A Human person can investigate them manually.

Figure 1. The proposed system approach, The camera captures the behavior, and the face is then captured and searched for a potential suspect

The system starts with the image acquisition phase (capture), followed by the stage of extracting the facial image from the overall image, then the phase of aligning and measuring the image (adjusting the angle of the face with the camera angle). Extraction of the essential features of the image is done to have better matching. The matching stage between the desired image and the picture store is executed. And finally issuing a report with the closest n images to the captured image [30–32].

The proposed algorithm goes through the following phases.

- Detection: Take the image either by binary images using electronic scanners or tri-dimension using camcorders.
- Alignment: After capturing the image, the system determines the position, size, and direction of the head. If the detection is done using the "3D" camcorder, it can select this even if the image is 90 degrees inside. If the image is two-dimensional, the bending between the face and the camera is about 35 degrees [33].
- Measurement: The system software calculates curves and aliases on the face accurately up to parts of the millimeter. This information was transformed into a face template and intended to extract distinguishing features in the physiological and behavioral characteristics of the template in the information databases [34].
- Representation: In this step, the system translates the template into a code composed of a set of numbers representing the characteristics of this template, where these codes are unique to each template.
- Matching: Where the manufacturers use the method of properties to compare the corresponding templates, that is, the development of an approved standard to determine the strength of any match. If the level of conformity exceeds the previously specified level, the process is considered a complete match. If the images in the databases are three-dimensional images, the matching process does not require any conversion to the image. If this two-dimensional displacement causes a challenge, the mold must be converted into two-dimensional images by using the logarithm in the words and then matching [35]

Authentication vs Identification:

Facial recognition systems seek to identify the identity of a person whose image we have, depending on the memory stored in these systems.

The memory of the face recognition system is formed and extracted from the training set, a set of pre-ordered images. Within this project, the training package consists of features vectors, extracted from a well-known set of faces for different suspects [36].

It is represented by the radial features, matrices, so to speak, selected from the original image matrices, representing the important and fundamental values within the original images, thus reducing the size of the images to the rays representing the image abstract.

Thus, the task of the recognition system lies in the process of finding the most similar and closest feature in the training group to the beam of the characteristics extracted from the image presented for the test, the image required to identify the owner through the identification system [37].

Here, within this system, we want to know and identify the identity of a person, by passing the image of this person to the system, in this case, this image is to be identified as the test image [31].

In order to extract the images from the images within this project, we will rely on one of the classification algorithms in the process of extracting the feature vector of the images.

A. Geometrical Method:

This method is based on the calculation of distances between the characteristics of the face such as the distance between the eyes and the distance between the line of the mouth and the line of the eyes and the distance between the center point of the nasal line of the mouth and the width of the eye, nose, and mouth [38].

The principal component analysis (PCA) is one of the most successful techniques used in image recognition and image compression. The main objective of the PCA algorithm is to reduce the large dimensions of the data space to spaces in smaller dimensions. Usually, the new spaces are the spaces of the features (containing the basic and important features of the data in their original spaces) [39].

Steps of the algorithm:

- The representation of each one of the following dimensions converted to a single beam with the following dimensions:

- The middle face is calculated through the following relationship:

$$\Psi = \frac{1}{M} \sum_{i=1}^{M} \Gamma_i \tag{1}$$

- Normalize each image beam by subtracting from the middle face as follows:

$$\Phi_i = \Gamma_i - \Psi \tag{2}$$

- The matrix formed:

$$A = |\Phi_1, \Phi_2 ..., \Phi_M| \tag{3}$$

- Calculate the variance matrix with the dimensions of the face variations after M2 × M2:
- Here we calculate the Vi rays of the AAT matrix, which is in the following relationship vi * ai (modifier) where ai is the original image. Reach this relationship by ATAvi = μivi And AAT (Avi) = μi (Avi)
- Calculate the ui rays of the AAT matrix using the relationship ui = Avi
- (DIMENSION OF DIMENSIONS): Each face is represented by only the values that correspond to the largest K values:

In the first row, a group of Eigenfaces (self-faces that agree with major self-values) is shown. The phrase "self-face" comes from the fact that self-rays look like phantom images.

1- Comparative process:

In the comparison process, all the previous steps of the image to match with the images in the database and calculate the distance between the images entered with the images in the database if they

The distance > threshold, the image is identical.

III. Pros And Cons

The pros of the system include [15]:

Suppression of crime:

This is the biggest and most impressive feature of the installation of surveillance cameras. Surveillance cameras can provide solutions if you have problems with theft, punctuality, or productivity. In addition to Homes and offices are no longer becoming easy targets for criminals.

Evidence Collection:

Having cameras installed in strategic places is handy when monitoring actions and words from people during an event. The clear images make the face flawless and are more efficient than ever in recording a series of events.

Access to the right decisions:

Screenshots from surveillance cameras can help you make correct and fair decisions when settling conflicts, whether in local scenarios. Whether you are dealing with a situation involving disputes within the family, between your employees, or between your customers and service personnel, you can put your doubts in comfort with the help of your camera.

Keeping records:

The records control system supports 24 hours / 7 days. So you are able to know what happened outside your home or office about two weeks ago. Additionally, You can hide your security logs. Record cameras and document everything they see regularly, according to the date and time of the event.

The cons include [15]:

Privacy issues:

There have been a few cases in the past where many surveillance cameras were attacked by hackers. In addition, there are cases in which staff is objected to ongoing monitoring without their

doi:10.20944/preprints202303.0120.v1

6 of 10

permission, and refer to "invasion of privacy" as a reason. A few have also taken legal action against their employers in this regard [40].

It is expensive:

The micro control system will cost hundreds, even thousands of dollars depending on the features, number of cameras, and surveillance systems, which you may need to purchase.

Can be vulnerable to hacking:

Technology may be understood by criminals who are tech-savvy and develop ways to disable/disconnect them from the power source.

In the worst case, hackers can run a security clutter with your camera system using the Internet and use it to spy on you instead. This makes security cameras vulnerable and/or misused.

Does not stop theft or crime:

Cameras enable users to record footage to watch later, which helps capture criminals and obtain justice from the law. You cannot stop the crime when it is in progress.

IV. Research Results

There is a lot of controversy in the present time about the legality of the spread of surveillance cameras in public places frequented by people in their daily lives. We believe that the cameras in government buildings, vital and public installations, security centers, airports, border crossings, and traffic control are designed to protect the homeland and the public interest, and the protection of the occupants of these places by putting these cameras in places prominent, visible, and open to the public, but may be considered hidden cameras in the places of entertainment, markets, hotels, restaurants and pedestrian paths that are an outlet for fun and relaxation people consider it as a kind of violation of privacy, in light of the lack of regulation for the installation of surveillance cameras and mode of operation and the mechanism for the protection and preservation of the recordings [41].

As mentioned above, legal regulations criminalize the placement of surveillance cameras in private places where visitors do not know they are being observed because of the violation of privacy as an inherent right that cannot be violated in any way through the publication of images and videos that affect the privacy of individuals or may lead To blackmailing them in one way or another as many homeowners, shops and facilities put surveillance cameras to protect their property without regard to the right of individuals not to violate their privacy, while they are in or passing through this special places [42].

On the other hand, we believe that the installation of surveillance cameras in the workplace requires the employee to know the existence of these cameras, which means acceptance of this and understanding the needs of the work such as the protection of banks, banks and jewelry shops and other facilities while protecting the employee's right not to use this evidence against them if put in a fraudulent manner without their knowledge. Failure to notify them of the existence of these cameras is a violation of their personal rights and freedoms. Such cameras may not be placed in toilets or places of rest, as there is no need for such violations [43].

We believe that surveillance cameras are considered complementary legal presumptions that are not taken as material evidence of the crime in general, except with the prior permission of the competent investigative authorities. On the other hand, such recordings may not be published during criminal investigations of crimes other than those concerned with the investigation, criminal images, or what is known as visual fingerprint, which has become one of the most important ways to identify the perpetrators in many of the various crimes in modern times.

We conclude that there must be strict control over the work of public surveillance cameras to ensure that this information is protected, that records are not infringed or used for personal purposes in any way, and to reduce the clutter of electronic eyes that have been planted in most hotels, restaurants, shops, and others. The right to privacy, organize the mechanism and methods of the development of these cameras and the purposes for which they were established, and the consent of the concerned

parties to license and provide the conditions and specifications and ensure the confidentiality of the information and alert visitors and visitors to these places the existence of these cameras in general.

Security cameras has the ability to interact with and respond to potential security threats. They can also provide a visible deterrent to would-be criminals and can assist in evacuation or other emergency situations [44]. They can also provide a personal touch to security and can be helpful in cases of customer service. A comparison of security cameras and human-based surveillance is provided in Figure 2.

Banks operating in the local market have recently stepped up their ATM development and security efforts as part of their efforts to control piracy risk and customer account violations, according to the assurance of IT and computer system specialists.
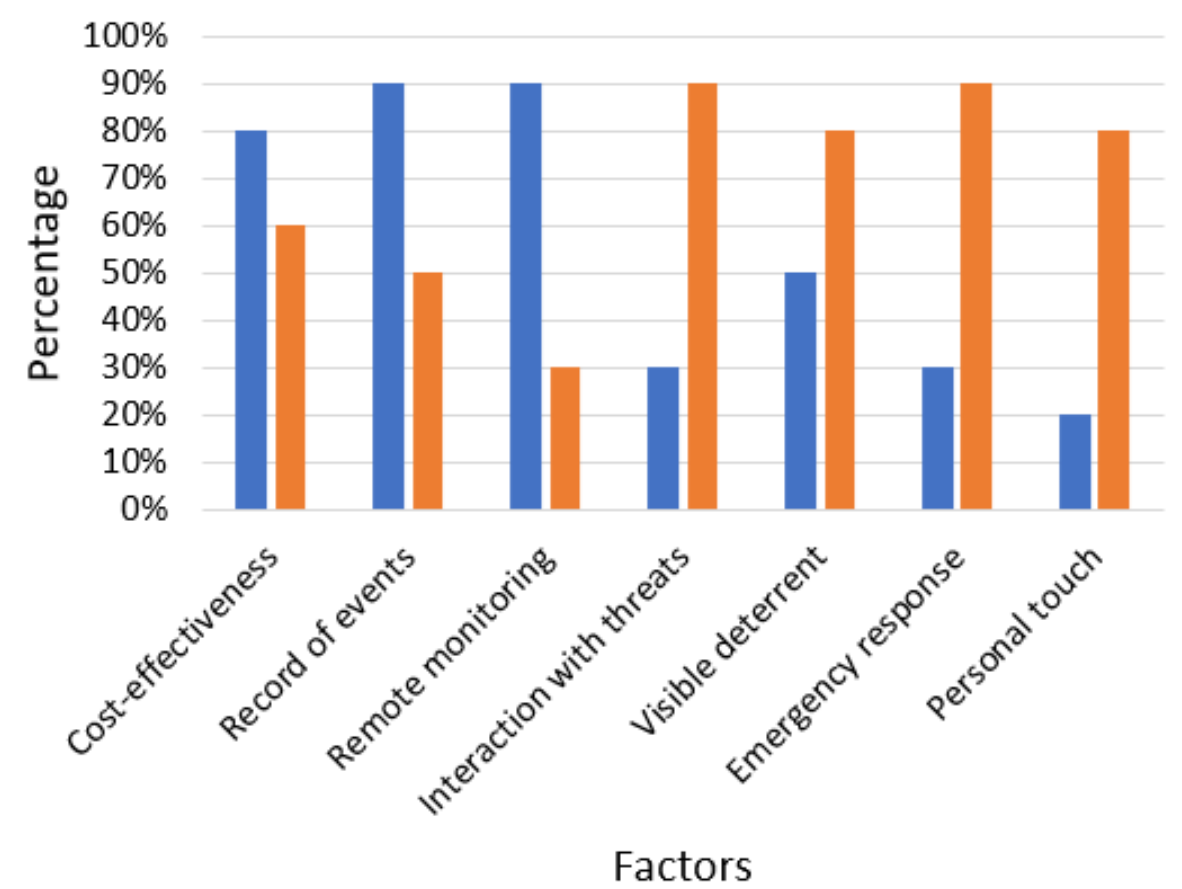

Figure 2. The comparison of the proposed approach with traditional human-based surveillance in bank ATMs

Experts believe that the most prominent preventive measures are to provide ATMs with self-monitoring cameras, which can automatically stop the process of withdrawal in the event of any illegal or suspicious actions. As well as the ability to identify users to ensure the possibility to stop dealing on accounts prone to theft quickly, in addition to the installation of some of the plastic parts in the introduction to the credit card segment, to prevent the installation of some devices used by pirates to copy data on the cards.

In the future reserves that should take to face violations of the confidentiality of customer accounts, and robbery of their assets, the banks put into their accounts good insurance and adequate ATM machines. Where it installed a number of surveillance cameras distributed thoughtfully to see all the entrances and exits of the cash withdrawal machine, as well as to intensify the security guard, to block any robberies that may be on the machines.

V. Conclusion and Future Work

We have considered the use of data mining to determine patterns of crime patterns using crime collection techniques. Our contribution here is to formulate crime pattern detection as a task for automated learning and thus. To be completed... As a future extension of this study, we will develop models for predicting crime missions [26] that will help to deploy police at potential crime sites most likely at any given time period to allow effective use of police resources. We also plan to consider the development of social networks to connect criminals, suspects, and gangs and to study their mutual relations. In addition, the ability to search for suspicious descriptions in the regional FBI databases, [30], for databases violation of traffic rules for different situations and not only at the ATM. To help detect the pattern of crime.

References

1. Abousamra, R.; Hosam, O. Quantitative Classification of Cognitive Behaviors for Industrial Projects' Managers in the MENA Region. 8th International Conference on Information Technology Trends (ITT. IEEE, 2022. doi:10.1109/itt56123.2022.9863957.

2. Hosam, O.; Abousamra, R. Enhancing Deep Training of Image Landmarking with Image CAPTCHA. 8th International Conference on Information Technology Trends (ITT. IEEE, 2022. doi:10.1109/itt56123.2022.9863967.

3. Hosam, O.; BinYuan, F. A Comprehensive Analysis of Trusted Execution Environments. 8th International Conference on Information Technology Trends (ITT. IEEE, 2022. doi:10.1109/itt56123.2022.9863962.

4. Hosam, O. An earthquake query system based on hidden Markov models. *International Journal of Embedded Systems* **2022**, *15*, 149–157. doi:10.1504/ijes.2022.10047935.

5. Hosam, O. Intelligent Risk Management using Artificial Intelligence. Advances in Science and Engineering Technology International Conferences (ASET, 2022, pp. 1–9,. pp., doi:10.1109/ASET53988.2022.9734861.

6. Hu, J.; Liang, W.; Hosam, O.; Hsieh, M.; Su, X. 5GSS: a framework for 5G-secure-smart healthcare monitoring. *Connection Science* **2021**, p. 1–23. doi:10.1080/09540091.2021.1977243.

7. Priadana, A.; Habibi, M. Face Detection using Haar Cascades to Filter Selfie Face Image on Instagram. 2019 International Conference of Artificial Intelligence and Information Technology (ICAIIT. IEEE, 2019, p. 6–9.

8. Liu, B.; Xiao, L.; Long, J.; Tang, M.; Hosam, O. Secure Digital Certificate-Based Data Access Control Scheme in Blockchain. *IEEE Access* **2020**, *8*, 91751–91760. doi:10.1109/access.2020.2993921.

9. Lei, Q.; Xiao, L.; Hosam, O.; Luo, H. A novel watermarking algorithm based on characteristics model of local fragmentary images. *International Journal of Embedded Systems* **2020**, *12*, 11–21. doi:10.1504/ijes.2020.105305.

10. Ali, M.; Jung, L.T.; Hosam, O. A new text-based w-distance metric to find the perfect match between words. *Journal of Intelligent and Fuzzy Systems* **2019**, *9*, 1–12,. doi:doi.org/10.3233/jifs-179552.

11. Hany, M.; Youssef, B.; Darwish, S.; Hosam, O. Intelligent Watermarking System Based on Soft Computing. International Conference on Advanced Intelligent Systems and Informatics; Springer: Cham, 2019; p. 24–34. doi:10.1007/978-3-030-31129-2_3.

12. Kumar, U.; Subash, S. ATM-Security using machine learning technique in IoT.

13. Hosam, O.; M, H. Modified Fast Gray Level Grouping Approach for Enhancing Image Contrast. *Journal of Theoretical and Applied Information Technology* **2019**, *97*.

14. Huang, W.; Li, R.; Xu, J.; Huang, Y.; Hosam, O. Intellectual property protection for FPGA designs using the public key cryptography. *Advances in Mechanical Engineering* **2019**, *11*, 16–22. doi:10.1177/1687814019836838.

15. Geitgey, A. Modern Face Recognition with Deep Learning. In *Medium Corporation*; Medium Corporation, 2016.

16. Hosam, O. Hiding Bitcoins in Steganographic Fractals. 2018 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT. IEEE, 2018. doi:10.1109/isspit.2018.8642736.

17. Hosam, O. Toxic Comments Identification in Arabic Social Media. *International Journal of Computer Information Systems and Industrial Management Applications* **2019**, *11*, 219–226.

18. Chen, Y.; Xiao, L.; Hosam, O. A Performance Evaluation Method of Coal-Fired Boiler Based on Neural Network. International Conference on Smart Computing and Communication; Springer: Cham, 2019; p. 277–285. doi:10.1007/978-3-030-34139-8_27.

19. Ahmad, M.H.; Hosam, O. Hybrid design for cloud data security using combination of AES, ECC and LSB steganography. *International Journal of Computational Science and Engineering (IJCSE* **2019**, *19*. doi:10.1504/ijcse.2019.100236.

20. Zhu, W.; Hosam, O.; Zheng, X. A secure hierarchical community detection algorithm. *International Journal of Computational Science and Engineering (IJCSE)* **2019**, *19*. doi:doi.org/10.1504/ijcse.2019.100245.

21. Gupta, H. Facial Similarity with Siamese Networks in Pytorch, Hackernoon October 14th 2019.

22. Liang, W.; Xie, Y.; Chen, X.; Hosam, O.; Chen. A Two-step MF Signal Acquisition Method for Wireless Underground Sensor Networks. *Computer Science and Information Systems* **2016**, *13*. doi:10.2298/csis160224019l.

23. Zhang, K.; Zhang, Z.; Li, Z.; Qiao, Y. Joint face detection and alignment using multitask cascaded convolutional networks. *IEEE Signal Processing Letters* **2016**, *23*, 1499–1503.

24. Hosam, O.; Ben Halima, N. Adaptive block-based pixel value differencing steganography. *Security Comm. Networks* **2016**. doi:10.1002/sec.1676.

25. Azriansyah, M.; Hartuti, N.; Fachrurrozi, M.; Tama, B. A Study about Principle Component Analysis and Eigenface for Facial Extraction. *Journal of Physics: Conference Series* **2019**, *1196*, 012010.

26. Eldén, L. Matrix methods in data mining and pattern recognition.

27. Hosam, O. Colored Texture Classification with Support Vector Machine and Wavelet Multiresolution Analysis. The IEEE Symposium on Signal Processing and Information Technology (ISSPIT'05, 2015. Abu Dabhi, UAE, doi:10.1109/isspit.2015.7394350.

28. Yu, B. Design and Implementation of Behavior Recognition System Based on Convolutional Neural Network. ITM Web of Conferences. EDP Sciences, 2017, Vol. 12, p. 01025.

29. Halima, N.B.; Hosam, O. Bag of Words Based Surveillance System Using Support Vector Machines. *International Journal of Security and Its Applications* **2016**, *10*, 331–346. doi:10.14257/ijsia.2016.10.4.30.

30. Team, C.S. Integration in the Cloud: Some Basics. In *Integration in the Cloud: Some Basics "*; online, 2015.

31. Bertinetto, L.; Valmadre, J.; Henriques, J.; Vedaldi, A.; Torr, P. Fully-convolutional siamese networks for object tracking. European conference on computer vision; Springer: Cham, 2016; p. 850–865.

32. Hosam, O.; Halima, N.B. A HYBRID ROI-EMBEDDINGBASED WATERMARKING TECHNIQUE USING DWT AND DCT TRANSFORMS. *Journal of Theoretical and Applied Information Technology* **2015**, *81*.

33. Halima, N.B.; Hosam, O. Embedding Image ROI Watermark Into Median DCT Coefficients. *IRECOS* **2015**, *10*. doi:10.15866/irecos.v10i6.6219.

34. Hosam, O. Car License Plate Localization Using Hole Filling and Support Vector Machine. *International Review on Computers and Software (IRECOS* **2014**, *9*. doi:10.15866/irecos.v9i10.2238.

35. Hosam, O.; Halima, N.B.; Dakroury, S.; Abdel-Rahman, E.O. RECONSTRUCTING, AUGMENTING AND MANIPULATING 3D SCENE FROM SEQUENCE OF IMAGES. *Journal of Theoretical and Applied Information Technology* **2017**, *73*, 12–17.

36. Hosam, O.; Malki, Z. Steganography Technique for Embedding Secure Data into the Image Regions with Abrupt Changes. *Life Sci J* **2014**, *11*, 126–130.

37. Liang, W.; Zhang, D.; You, Z.; Li, W.; Hosam, O. A Survey of Techniques for VLSI IP Protection. *Information Technology Journal* **2013**. published June 12, 2013., doi:10.3923/itj.2013.

38. Hosam, O.; Alraddadi, A.S. Novel Image Watermarking Technique Based on Adjacent Pixel Position Switch. *JNIT* **2013**, *4*, 81 88,. doi:10.4156/jnit.vol4.issue3.10.

39. Hosam, O. Side-Informed Image Watermarking Scheme Based on Dither Modulation in the Frequency Domain. *The Open Signal Processing Journal* **2013**, *5*, 1–6. doi:10.2174/1876825301305010001.

40. O. Hosam, W.; Youssef, B.A.; Abdou, M. Public Watermarking Scheme for 3Ds Laser Scanned Archeological Models. The Seventeenth IEEE Symposium on Computers and Communications (ISCC'12); Cappadocia: Turkey, 2012. doi:10.1109/iscc.2012.6249326.

41.　　Hosam, O.　Motion Compensation for Video Codec Based on Disparity Estimation.　The Seventeenth IEEE Symposium on Computers and Communications (ISCC'12); Cappadocia: Turkey, 2012. doi:10.1109/iscc.2012.6249355.

42.　　O. Hosam, X.S. Stereo Image Reconstruction Using Adaptive Window Approach. the proceeding of 2nd International Conference on Advanced Computer Theory and Engineering, ICACTE2009, 2009, p. 33–41. doi:10.1115/1.802977.paper4.

43.　　Hosam, O.; Yang, L.; Liang, W.; Sun, X.　Watermarking 3D Triangular Mesh with High Visual Quality. *JDCTA: International Journal of Digital Content Technology and its Applications* **2010**, *4*, 107 116,. doi:10.4156/jdcta.vol4.issue4.11.

44.　　O. Hosam, X.S. Three Dimensional Reconstruction Using Enhanced Shape From Stereo Technique. the proceeding of "2009 Eight IEEE/ACIS International Conference on Computer and Information Science", 2009, p. 627–632.　doi:10.1109/icis.2009.166.