

How to cite this article:

Rashid, A. M., Yassin, A. A., Alkadhmaewee, A. A., & Yassin, A. J. (2020). Smart city security: Face-based image retrieval model using gray level co-occurrence matrix. *Journal of Information and Communication Technology, 19*(3), 437-458.

SMART CITY SECURITY: FACE-BASED IMAGE RETRIEVAL MODEL USING GRAY LEVEL CO-OCCURRENCE MATRIX

¹Abdullah Mohammed Rashid, ²Ali Adil Yassin,

¹Ahmed Adel Abdel Wahed & ²Abdulla Jassim Yassin

¹Education College for Human Science, University of Basrah, Iraq

²Computer Department, University of Basrah, Iraq

Abdalla_rshd@yahoo.com;

aliadel79yassin, ahmedadel1949, abdullajas@gmail.com

ABSTRACT

Nowadays, a lot of images and documents are saved on data sets and cloud servers such as certificates, personal images, and passports. These images and documents are utilized in several applications to serve residents living in smart cities. Image similarity is considered as one of the applications of smart cities. The major challenges faced in the field of image management are searching and retrieving images. This is because searching based on image content requires a long time. In this paper, the researchers present a secure scheme to retrieve images in smart cities to identify wanted criminals by using the Gray Level Co-occurrence Matrix. The proposed scheme extracts only five features of the query image which are contrast, homogeneity, entropy, energy, and dissimilarity. This work consists of six phases which are registration, authentication, face detection, features extraction, image similarity, and image retrieval. The current study runs on a database of 810 images which was borrowed from face94 to measure the performance of image retrieval. The results of the experiment showed that the average

precision is 97.6 and average recall is 6.3. Results of the current study have been relatively inspiring compared with the results of two previous studies.

Keywords: Image retrieval, image similarity, extracted features, smart city, security.

INTRODUCTION

Population growth has become one of the most interesting topics for researchers and practitioners, they show that the percentage of populations in modern cities is 54% while in the rural areas is 46%, and the increase in urban cities will rise to 66% at the beginning of 2050 (Makrushin & Dashchenko, 2016). In order to address population growth in urban centers, the idea of using communication and technology is emerging to reduce costs and create a more livable urban environment. The use of sensors, technology, and communication in cities has led to the use of the new term “smart city.” Smart city has been defined as the use of communication technology to collect data which is used to integrate key information of core systems running cities; which makes intelligent responses to the different needs of its residents, including managing transportation systems, traffic, water supply networks, and others (Qin et al., 2010). When cities become smarter, a series of security breaches are expected because of the vulnerabilities of smart city applications (Biswas & Muthukkumarasamy, 2016; Martínez-Ballesté et al., 2013). Therefore new trends of smart city security have emerged to counter smart city threats (Gharaibeh et al., 2017). Energy system monitors energy generation by using a set of sensors to analyze collected data. Zanella et al. (2014) focused more attention on the Internet of Things (IoT) and surveyed the most important protocols and technologies related to smart cities in Padova, Italy. The main findings characterized in their survey revealed that most smart cities employed the same features in technologies. For instance, the vehicle monitoring system observes roads and collects car information regarding city security. The smart environment monitoring system uses sensors to collect data about the environment so as to create a suitable climate and sustainable environment for the smart cities. In this study, we present a secure scheme to retrieve images from smart city servers to identify wanted criminals by using Gray Level Co-occurrence Matrix (GLCM).

The proposed scheme extracts only five features of query images which are: contrast, homogeneity, entropy, energy, and dissimilarity. This work consists of six phases which are registration, authentication, face detection, features extraction, image similarity, and image retrieval. The main contribution of this research is to develop a scheme for image similarity and document

retrieval. The proposed scheme is developed based on the critical analysis of image matching factors in a smart city environment, which could indicate a reliable project to implement in government centers such as a police station. In this study we improved on smart city security, enhanced the performance of police stations and the competitiveness of smart city services. There are many benefits that can be gained from the proposed scheme such as providing a method to efficiently identify wanted criminals through checking their images and retrieving related documents. The rest of this paper is organized as follows: the related works are summarized in the second section and the proposed phases in the scheme are presented in the third section. The fourth section focuses on the experimental design and results analysis. We run the proposed scheme and study its performance and efficiency in the fifth section. Finally, the sixth section presents the conclusion and future work.

RELATED WORK

In this section, we present a brief overview of existing research in the field of image retrieval and smart city security. In recent years the terms, smart cities, remote sensing, and observation technologies have been bandied about and frequently this question would pop up, what is a smart city? A smart city is an urban area that utilizes too many kinds of electronic sensors to aggregate data which is the main source to manage the assets of smart cities and its resources efficiently (Gracia & García, 2018; McLaren & Agyeman, 2015). Smart cities have different approaches to collect data from devices, citizens, and assets that are used to conduct analysis, make decisions, control transportation systems, power plants, traffic, water supply networks, law enforcement, information systems and others (Gracia & García, 2018; Musa, 2016). Smart city security has become one of the most important issues required to keep residents and their assets secure (Kumar et al., 2016). Smart cities use different information systems to provide a high quality of life for its citizens in a clean, energy efficient and climate-friendly urban environment (Bartoli et al., 2011). Smart cities cannot be smart without information systems, databases, and technology (Bartoli et al., 2011). This explains why several information systems are running concurrently to make the life of local residents easier because of the services provided. This research focuses on one of these information systems which is image retrieval and its role in maintaining the safety of city residents. In the next section, we present different techniques, algorithms, and studies on image retrieval.

GLCM was used to retrieve documents from a data set (Dixit & Shirdhonkar, 2018). This approach utilized three algorithms to extract document images, perform features extraction, and retrieve documents. As a

result, it achieved 82.66 as average precision and 26.8 as average recall. This study suffered from response time because the number of retrieved documents was 20 which required a long time to react (time-consuming). This issue was solved by minimizing the number of retrieval images and documents to support response time. Thus, Dixit and Shirdhonkar (2018) proposed a new method for document retrieval based on features extracted from face biometrics. Their study used only three phases to retrieve documents which were: (1) extraction of personal images from query documents (2) extraction of personal image features and (3) retrieval of documents with image features. The efficiency of the proposed method was measured by average precision and average recall which were 67.15 and 16.52, respectively. This study experienced a fundamental issue which was that query documents already contained personal images and personal information. Document information such as name, ID, and numbers were easy to search and retrieve in databases as these documents contained similar information. Thus, the current study uses an online camera to capture personal images, and then request that all documents have the same image features.

Du et al. (2020) presented a fast and secure scheme for image retrieval by using deep hashing algorithm. This work combined block 4-D hyperchaotic system and DNA sequence to encrypt examined images. This experiment of the proposed scheme was run on CIFAR-10 dataset which contained 1000 images and the retrieval efficiency achieved was 0.8931 which was considered as impressive. Thus, the current research consists of generating a once dynamic Token (TK) from the hash table used to encapsulate a shared key (SK) before sending to the Police Office (PO) in addition, image features are retrieved images which are sent to the PO encrypted. There were also several studies developed based on neural networks to retrieve images. The fuzzy hybrid learning algorithm was used as a neural network for image recognition and retrieval (Haddadnia et al., 2003). The current study proposes a new algorithm for system learning that offers faster convergence, less sensitivity and the average precision achieved in this study is estimated at 99.55%.

Huang et al. (2018) argued that the performance of image retrieval depended on database size, database structure, and index file, which was the result of a study employing Neural Networks to develop MRBDL framework for image retrieval. The deep hashing on neural networks to force remote sensing to make correct decisions on image retrieval was conducted by Huang et al. (2018) and Wang et al. (2016) which trained neural networks to retrieve images and implemented developed frameworks from databases of animals, buildings and other objects. Li et al. (2018) employed deep hashing neural networks (DHNNs) to train remote sensing for image retrieval and examined images from general satellite databases. The proposed sensing showed sufficient results in comparison with other studies.

Image processing has been employed in different fields such as health and education to serve the world residents; for example, image processing and artificial intelligence or image processing and information system. Liliana et al. (2020) developed an artificial intelligent model analyzing facial expressions by using image features such as intensity, opened eyes, texture, histogram, and wrinkles which are used to investigate human emotions to better understand human interactions.

Ahmad et al. (2018) used an efficient method for image optimization, deep learning technique, and feature extraction to retrieve required images. The main secret of features extraction in this study was removing the background of images for better selection which led to accurate image detection. This study was run on a large database consisting of different categories such as vehicles, animals, and rivers. Meng et al. (2016) presented features extraction method to retrieve images. This study ran on different databases and resulted in high levels of accuracy. The main weakness of this study was that the results were not realistic for some objects. Moreover, the image optimization technique was not suitable for all images. Finally, based on the review of the literature, it can be seen that the implementation of image retrieval in smart cities has received less attention compared with other fields of technologies. Thus, the current study intends to address the gap through a new proposed scheme to support smart city security based on image retrieval. The experimental results of this proposed scheme showed an average precision of 97.6 and an average recall of 6.3.

Proposed Scheme

Our proposed scheme is composed of six phases: registration, authentication, detection, features extraction, similarity, and retrieval phase. Registration is the first phase to collect Police Officer (PO) information such as username (US), password (PW), fingerprint features (FPF), and police station address (PSA). The second phase is the Authentication Phase (AP) for recognizing the user's identity. It is a process of associating a received request with a set of identifying credentials collected in the registration phase. The credentials provided are compared to the records saved in a database of the authorized user's information in the cloud service provider (CSP). The third phase, the Detection Phase (DF) is the name for a set of mathematical methods for identifying personal faces in digital images which can be used for object detection and classification. This is to reduce the digital file size while preserving the value of the image. In the fourth phase, the Features Extraction Phase (FEP) is used to convert the huge amounts of pixels into numerous content features that enable efficient image classification of data images gathered from multiple sources. In the fifth phase, the Similarity Phase (SP) is an assessment process of an image matching ratio; images are often compared with a dataset of images to find the required images. Finally, in the sixth phase, the Retrieval Phase (RP) is

associated with the assessment results to send the highest similarity in images to the PO .

Registration Phase

Registration is the initial stage conducted to aggregate the *PO*'s information. The information gathering (*US, PW, FPF, PSA*), is used to identify the *PO*'s identity and to evaluate permission to access the *CSP*. Registration aims to create a record related to each *PO*. Figure 1 shows the details of the registration phase. The main steps of this phase are summarized in Algorithm 1.

Algorithm 1: PO registration

INPUT: Email, username, password, and fingerprint

OUTPUT: Complete the registration of PO

Step 1: Begin.

Step 2: PO has to provide a valid email to the CSP to verify the PO.

Step 3: CSP checks the email against the availability of the email.

Step 4: CSP asks the PO to submit a piece of information where the email is available, otherwise asks for another email.

Step 5: PO submits the US, PW, and PSA.

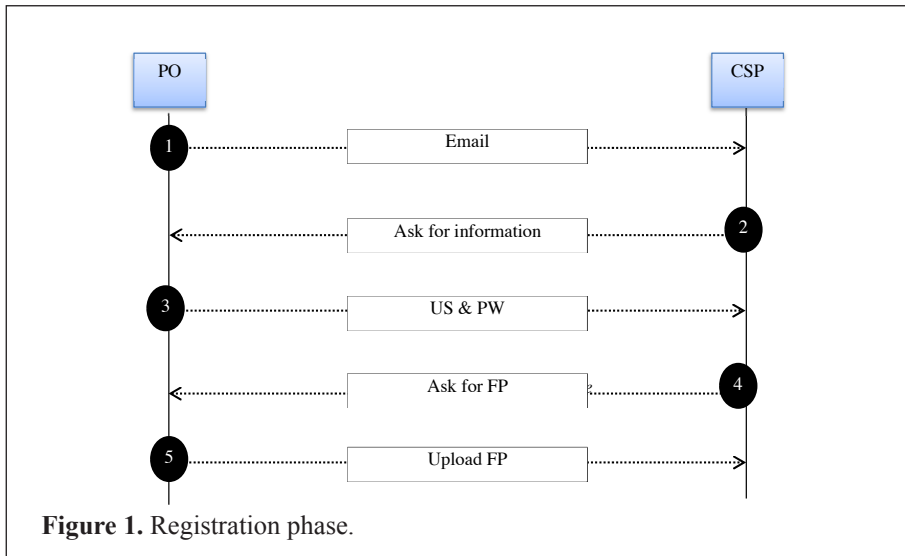
Step 6: CSP sends a request to upload the PO's fingerprint (FP).

Step 7: PO uploads the FP.

Step 8: CSP extracts the FPF, then stores it in the database.

Step 9: CSP confirms the completion of the registration phase.

Step 10: End.



Authentication Phase

This phase is divided into two sub-phases which are the handshaking phase and authorization phase. The main steps of this phase are summarized in Algorithms 2 and 3:

Algorithm 2: Handshaking phase

INPUT: Username and password

OUTPUT: Police officer authentication

Step 1: Begin.

Step 2: PO_i should submit his US_i and PW_i to CSP.

Step 3: CSP checks the validity of US_i, PW_i with the stored information which is initialized in the registration phase (RP).

Step 4: After approving the differences in US_i & PW_i , the CSP generates a once dynamic token (TK) from the hash table, that is used to encapsulate a shared key (SK) before sending it to the PO's email or SMS as shown in Equation 1 and Figure 2.

Step 5: PO_i checks the email and mobile to decapsulate the received token, before obtaining the SK for further authentication as shown in Equation 2 and Figure 3.

Step 6: PO has to enter the SK value in the login interface for authentication process.

Step 7: End.

Algorithm 3: Authorization

INPUT: FP

OUTPUT: Access to server resources

Step 1: Begin.

Step 2: CSP requests PO_i to send FP.

Step 3: PO_i uploads his FP, which is stored in flash memory or mobile memory.

Step 4: CSP extracts the FP's features, then checks by matching the FPF with the fingerprint features stored in the database.

Step 5: After approving the matching of FPF, CSP sends a secret key ($SK \in \mathbb{Z}_{n^+}$) to PO_i which is required in the retrieval phase.

Step 6: Finally, CSP provides PO_i an access to the server resources.

Step 7: End.

$$SK_i = \sum_{i=1}^n \text{Ascii}(US_i) \quad TK' = EnQ_{(TK)}(SK_i) \quad (1)$$

Where,

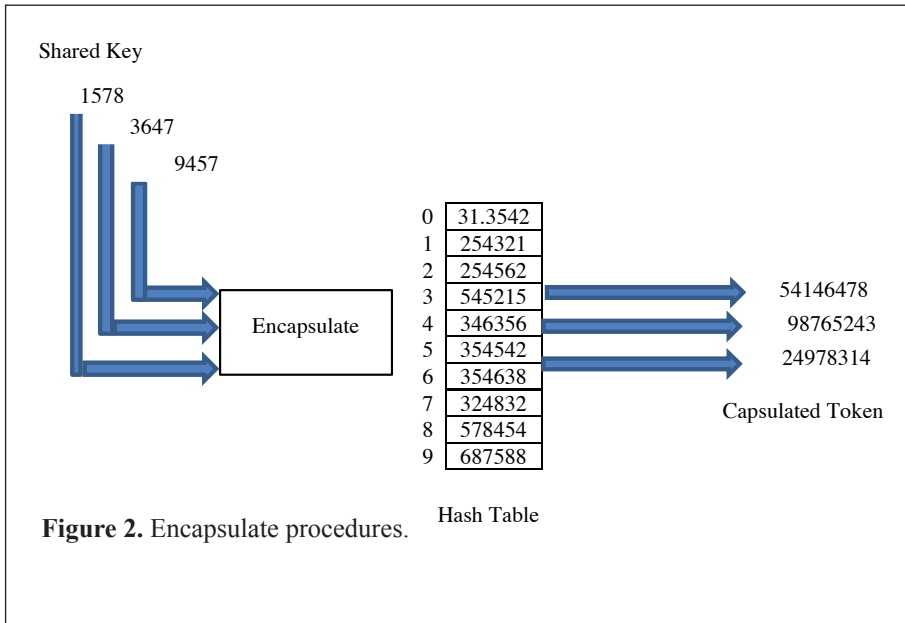
SK_i = Shared Key
 US_i = User Name
 TK' = Capsulated Token
 TK = Dynamic Token
 EnQ = Encapsulate Method

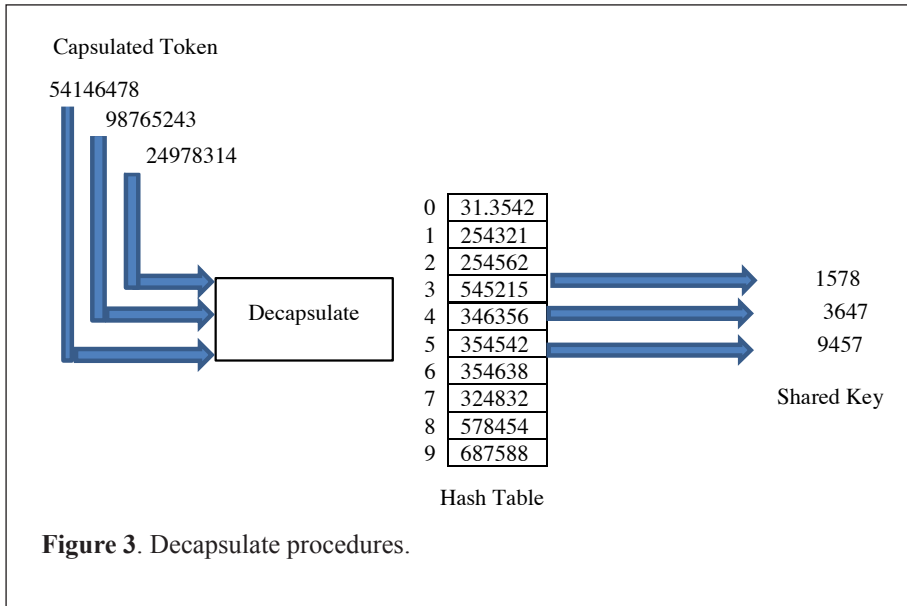
(2)

$$TK'' = DeQ_{(TK')} (SK_i)$$

Where,

TK'' = Decapsulated Token
 TK' = Capsulated Token,
 SK_i = Shared Key
 TK' = Capsulated Token
 DeQ = Decapsulate Method





Face Detection Phase

Face detection phase focuses on personal face discovery inside a digital image, which means examining an image to identify whether there is a certain person's face and where this face is located. This is to design a robust system for image classification based on object detection. Image classification depends on detected facial features which are compared with those stored in the database, as shown in Figure 4. The main steps of this phase are summarized in Algorithm 4.

Algorithm 4: Face detection

INPUT: The digital camera and examined persons

OUTPUT: Face extraction

Step 1: Begin.

Step 2: PO uses an online digital camera for capturing an image.

Step 3: PO only uploads personal face in the standard template.

Step 4: Identify the detected face.

Step 5: Transmit the identified face into the extraction phase.

Step 6: End.

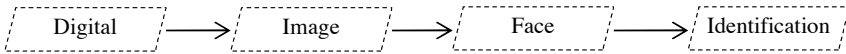


Figure 4. Face detection.

Features Extraction Phase

Features extraction is a set of methods, algorithms, and processes to collect several variables from a huge amount of data to simplify the description, classification, and similarity ratio of an image. Texture feature analysis helps to find the unique features for accurate classification of an image. There is a set of features grouped under texture analysis, terms such as: correlation, spatial frequency, inverse, angular, average gray level, and entropy.

GLCM is a method used to implement texture analysis to extract image features. GLCM is a matrix where the number of rows and columns is equal to the number of gray levels. First, divide the gray level image to n-intensity levels by means of intensity maps. A number of intensity levels in the image decide the size of the GLCM. Each element of the matrix at position (i, j) represents the frequency of co-occurrence of two pixels with intensity i and j, respectively, separated by a distance 'k' in the direction specified by a displacement vector (da Silva Torres & Falcao, 2006; Dixit & Shirdhonkar, 2018). Only five features are extracted from an image in this study which is contrast, homogeneity, entropy, energy, and dissimilarity. Finally, GLCM works based on Algorithm 5:

Algorithm 5: GLCM

INPUT: RGB Image

OUTPUT: GLCMR, GLCMG, GLCMB

Step 1: Begin.

Step 2: Separate RGB image to three channels which are R, G, and B.

Step 3: Divide each channel to 8- intensity levels.

Step 3 Find the GLCM for each level to come up with three matrixes which are GLCMR, GLCMG, GLCMB which are used to extract the factors.

Step 4: F1=GLCMR.....(factor 1)

F2=GLCMG.....(factor 2)

F3=GLCMB(factor 3)

F4=GLCMB(factor 4)

F5=GLCMB.....(factor 5)

Step 5: End.

These five factors are sent as a string to a similarity phase which is responsible for checking the percentage of similarity as shown in Equation 3.

$$F = F1 + F2 + F3 + F4 + F5 \quad (3)$$

Where,

F1=First factor

F2=Second factor

F3=Third factor

F4=Fourth factor

F5=Fifth factor

Image Similarity Phase

After distinguishing the image features of each face, the next step is to recognize the identities of the targeted face. The targeted face similarity is checked by comparing its features to the features of each face stored in the database. There are several studies conducted to check image similarity in order to achieve the classification. Image classification means identifying the distance between the examined face(s) and the database images. The main steps of this phase are summarized in Algorithm 6 and shown in Figure 5.

Algorithm 6: Image similarity

INPUT: Examined image

OUTPUT: The queue of similar images

Step 1: Begin.

Step 2: Let $EI = \{img_j\}$ where EI denotes the examined image.

Step 3: Let $DI = \{img_1, img_2, img_3, \dots, img_n\}$ where DI denotes the database image.

Step 4: Let $D(i, j)$, means a distance between two images, img_i and img_j which depend on examined features.

Step 5: Based on the results of distance function, $D(i, j)$.

Step 6: Database images are ranked, which creates a queue of images from high similarity to low similarity $QI = \{img_{h1}, img_{h2}, img_{h3}, \dots, img_{hn}\}$, QI denotes queue image, and H index means the similarity in ranks.

Step 7: Finally, redirect the QI to the retrieval phase which is responsible for passing the top image(s) to the PO as shown in Figure 5.

Step 8: End.

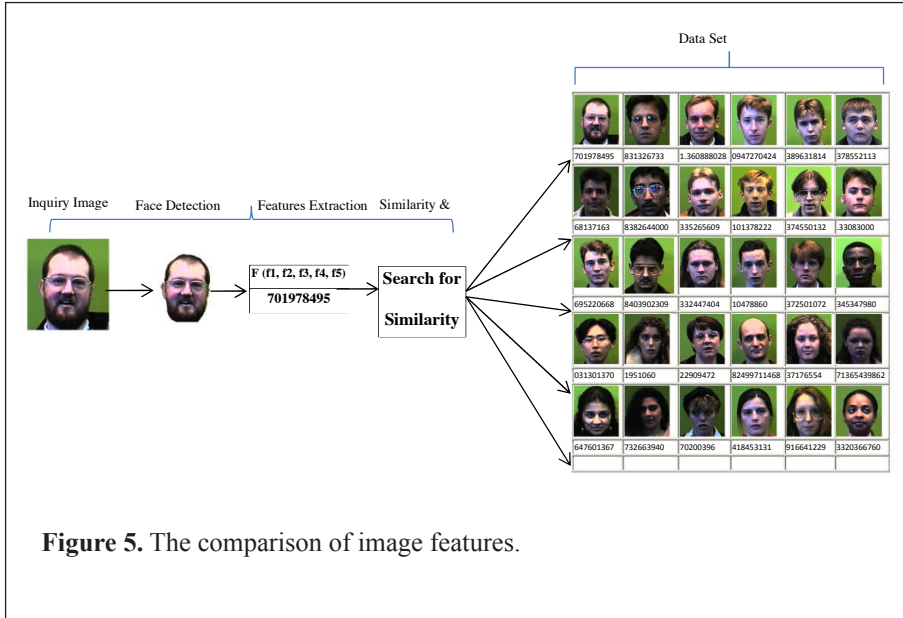


Figure 5. The comparison of image features.

Image Retrieval Phase

Image retrieval phase plays a core role in our scheme which is defined as processes to collect an image(s) with the highest similarity ratio to send to *PO*. This phase receives $QI = \{img_{h1}, img_{h2}, img_{h3}, \dots, img_{hn}\}$ from the similarity phase, and only selects the top three images which are in the start of the queue and sends to *PO*. The main steps of this phase are summarized in Algorithm 7 and Figure 6.

Algorithm 7: Image retrieval

INPUT: The queue of similar images

OUTPUT: Pass the documents to *PO*

Step 1: Begin.

Step 2: CSP retrieves the top three images and sends to *PO*.

Step 3: *PO* uses the secret key and fingerprint to decrypt the retrieved images.

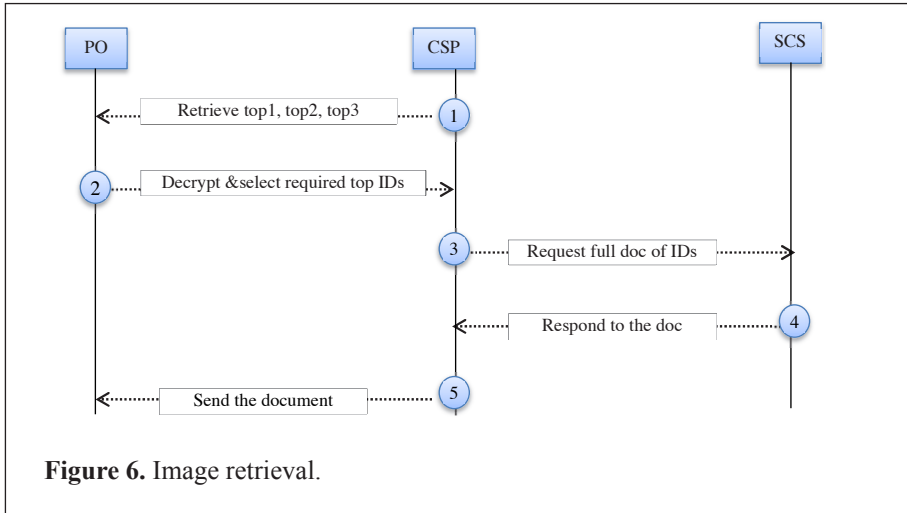
Step 4: *PO* selects the required image(s).

Step 5: CSP sends the selected image ID(s) to Smart City Servers (SCS)

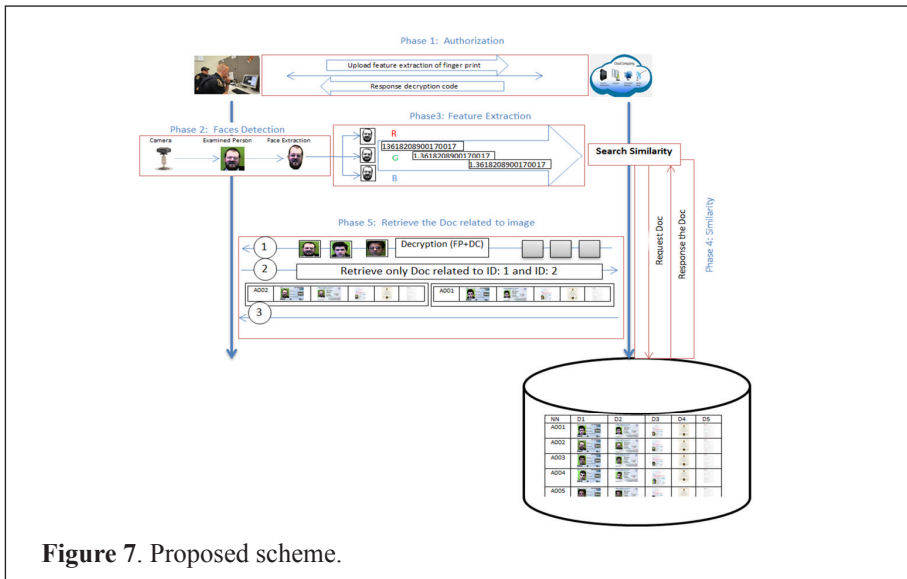
Step 6: SCS sends the full documents of required ID(s) to CSP.

Step 7: CSP sends the documents to *PO*.

Step 8: End.



Finally, Figure 7 shows the proposed scheme with six phases: registration, authentication, detection, features extraction, similarity, and retrieval. First phase—registration to collect the PO information. Second phase—authentication to ensure only the authorized PO can access the CSP database and check for image similarity. Third phase—face detection to upload personal image(s) into the proposed system. Fourth phase—features extraction to create a database of features. Fifth phase—check the similarity between query image(s) and database features, and the sixth phase, retrieval phase to retrieve top images to send to *PO*.



EXPERIMENTAL DESIGN AND RESULTS ANALYSIS

Experimental Results

In order to evaluate the performance of our proposed scheme regarding the search efficiency, we ran the proposed scheme on a real image database of face94 constructed by Dr. Libor Spacek which has 27 classes of an image. Our experiments were conducted on a 2.5 GHz Intel i7- 6500U processor; with a Windows 10 operating system of 64-bits, and 8 GB RAM (Lenovo Laptop). Furthermore, we used Java NetBeans IDE 8.0.2 to run our experiments.

Database Structure

The first step of the proposed scheme was creating a database of extracted features by using the 810-color images, which classified into 27 classes—16 classes for men and 11 classes for women. Each member was related to five documents. The total size of the database is computed in Equation 4.

$$Database\ size = \frac{810\ image}{30\ member} * 5\ doc \quad (4)$$

The extracted features of these images were contrast, homogeneity, entropy, energy, and dissimilarity. The documents related to the database of members were: passport, identification card, driving license, certificate, and work ID. Figure 8 shows a sample of the documents related to the database image.

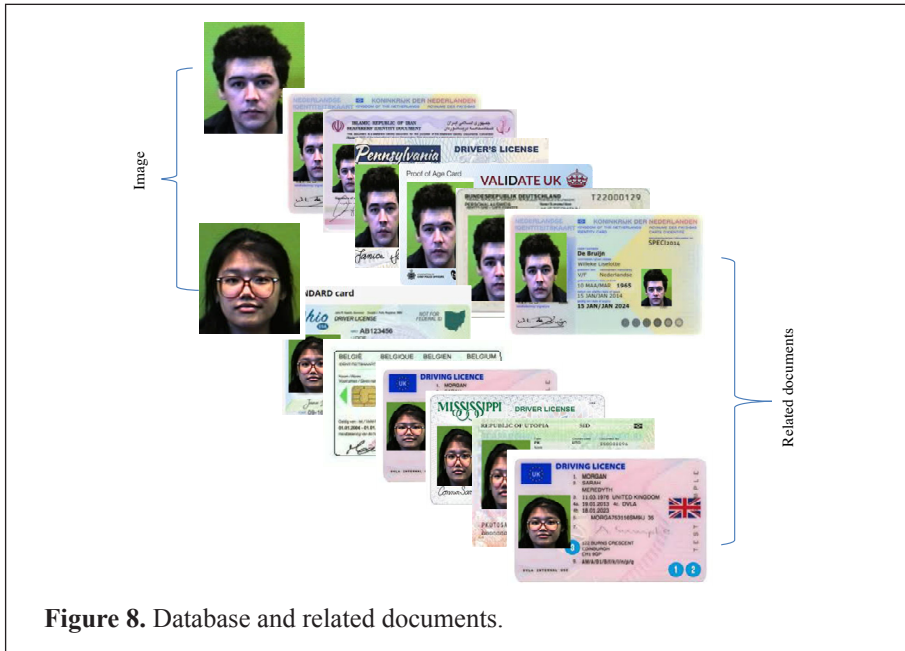


Figure 8. Database and related documents.

The database creation time differed, depending on the database size, the first 10 classes was created in 12 seconds, the second 20 classes was created in 64 seconds and the total number of classes which was 27 was created in 119 seconds as shown in Figure 9.

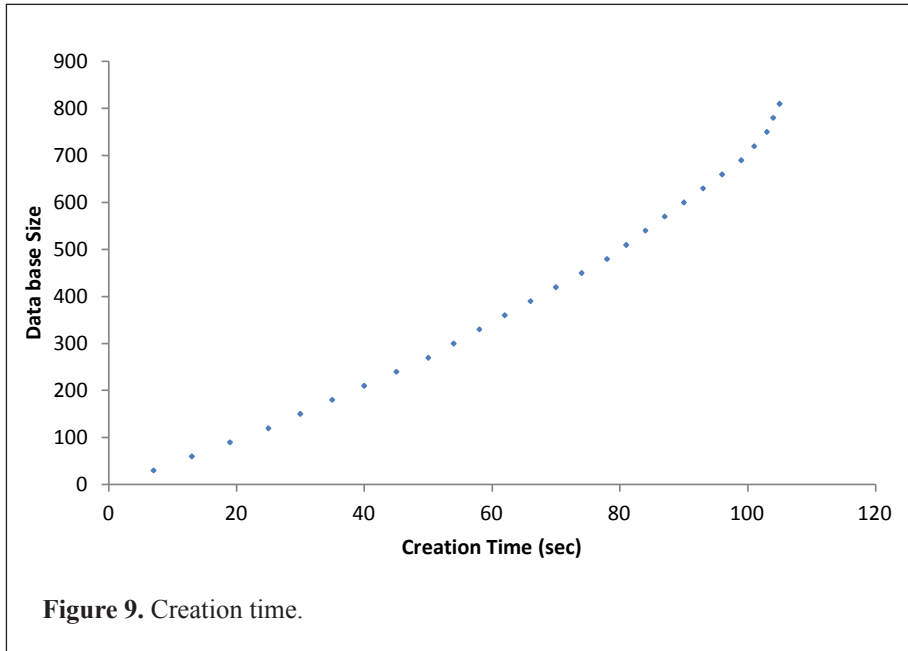
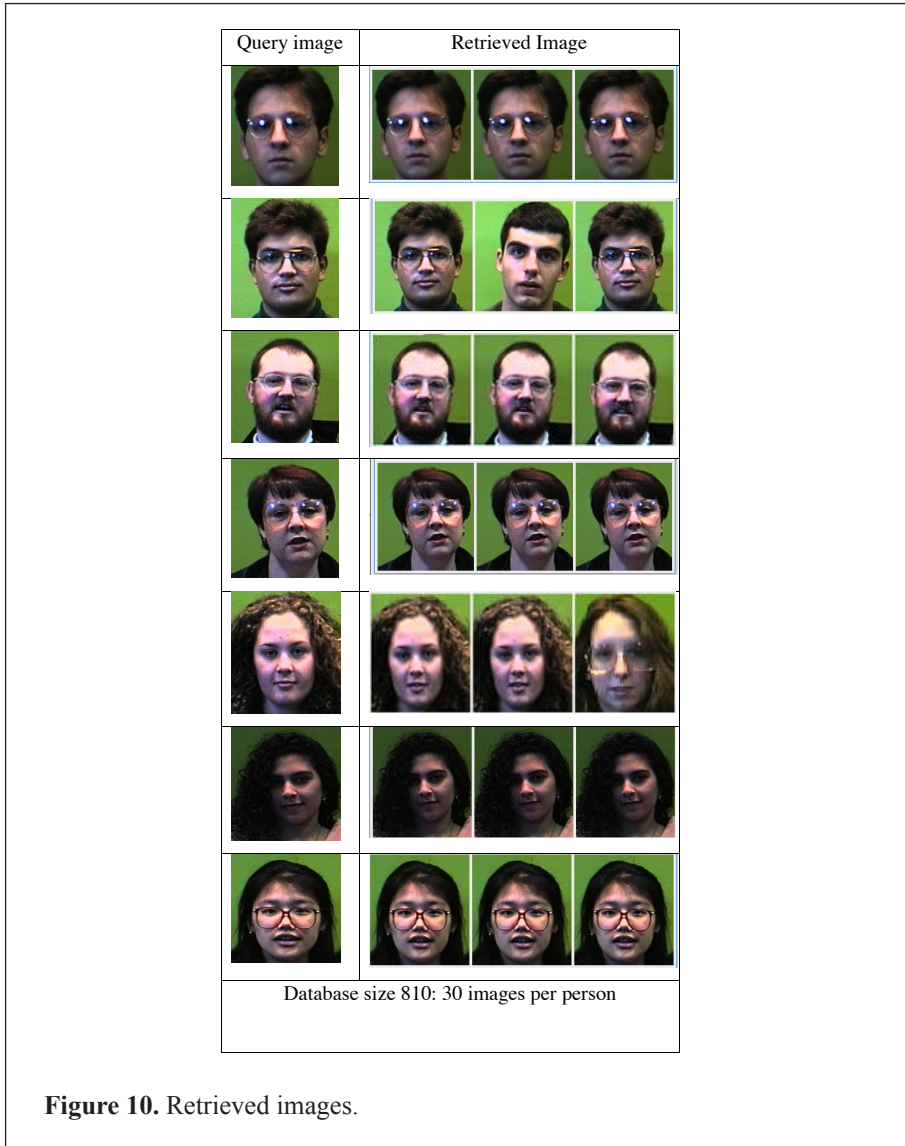


Figure 10 shows the retrieved images for the requested image using the proposed scheme. The proposed model retrieved exactly what was requested by the image where the database size was 810 images. This was because there were only 30 images for each person. The proposed model retrieved some different images which were related to scheme accuracy, precision and recall as computed in the following sections.



The evaluation of our proposed scheme was conducted by computing the precision, recall and f-measure for retrieved samples of images and related documents. Average precision is a measure of relevant images retrieved to the total number of images retrieved as shown in Equation 5.

$$\text{Precision} = \frac{\text{relevant images retrieved}}{\text{total number of images}} \quad (5)$$

Average recall is relevant images retrieved to the total number of relevant images in the database as shown in Equation 6.

$$\text{Recall: } \frac{\text{relevant images retrieved}}{\text{total number of images in DB}} \quad (6)$$

F-measure is the harmonic mean of precision and recall, as shown in the following Equation 7.

$$F - \text{measure} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad (7)$$

Table 1 shows the result of image similarity and document retrieval by using the proposed scheme. The average precision is 97.66; the average recall result is 6.3 and the F-measure is equal to 11.7. The result presented in Table 1 is evidence of the performance of the proposed scheme. Top1 means the highest matching result to the inquiry image which decreases gradually to Top 3. Table 1 confirms that the implementation of the proposed scheme in the smart city will help the police to catch criminals because it shows high similarity in results. Table 2 presents the comparison of results with previous studies which proved that the proposed scheme has met high levels of precision and recall. The result in Table 2 confirms that the proposed scheme reached a high similarity point in the current study. Figures 11 and 12 present a comparison of results of the current proposed scheme with other studies in the field of image retrieval.

Table 1

Results of Proposed Scheme

No.	DB Size	No. of image per person	No. of image retrieved	Evaluation Parameter	Top 1	Top 2	Top 3	Mean
1	810	30	3	Average precision	100	98	95	97.6666667
2	810	30	3	Average recall	3.3	6.2	9.5	6.33333333
3	810	30	3	F-Measure	6.38915779	11.6622	17.2727273	11.77469106

Table 2

Comparison of Proposed Scheme with Previous Studies

No.	Similarity Method	DB Size	No. of image per person	No. of image retrieved	Evaluation Parameter	Mean
1	Proposed Scheme	810	30	3	Average precision	97.66
					Average recall	6.34
					F-Measure	11.77
2	Dixit and Shirdhonkar (2017)	810	30	20	Average precision	67.15
					Average recall	16.52
					F-Measure	23.798
3	Dixit and Shirdhonkar (2018)	810	30	20	Average precision	82.66
					Average recall	26.19
					F-Measure	35.966

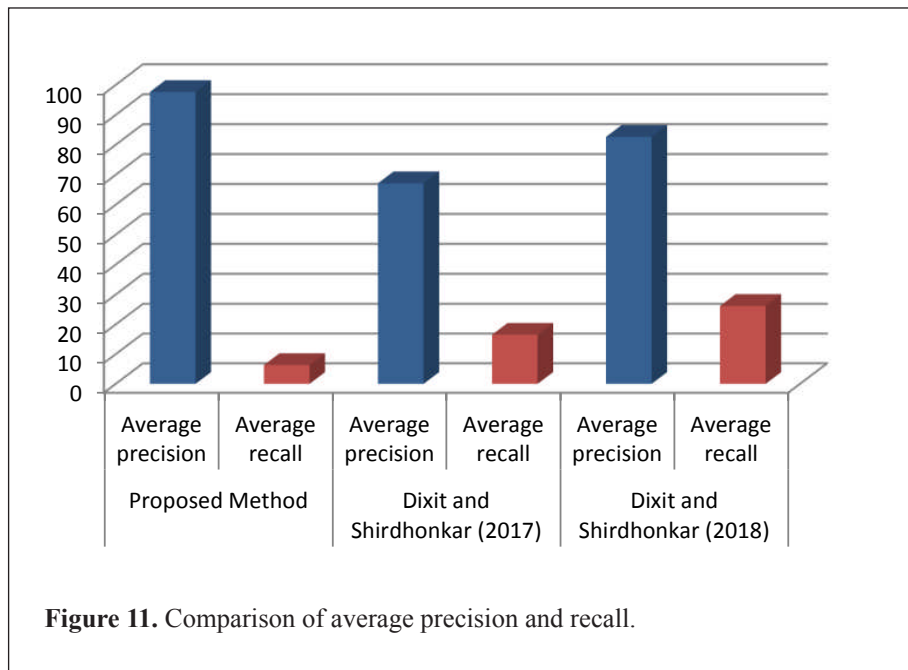


Figure 11. Comparison of average precision and recall.

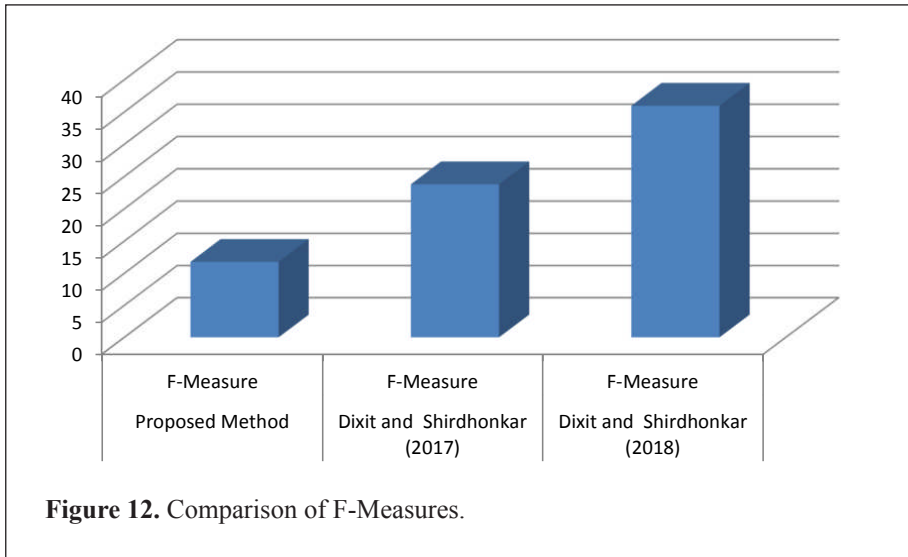
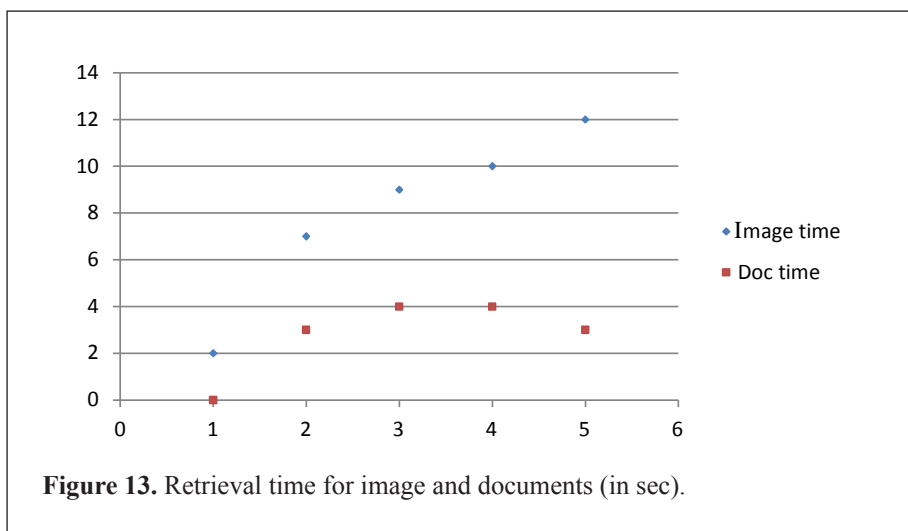


IMAGE RETRIEVAL TIME

The efficiency of the proposed scheme was measured through first, computing the retrieval time of the required images and then documenting them (Haralick et al., 1973; Wang et al., 2016). Retrieval time was considered in the design of this scheme because of the fast response techniques related to the well designed and researching strategies of the query images. Figure 13 shows the retrieval time according to the proposed scheme.



CONCLUSION

Admittedly there are some challenges in smart city security such as in identifying outsiders and criminals. This is because there has yet to be developed a study which reached 100% in terms of performance and efficiency of image matching in real time. This study proposes a new scheme to check for image similarity and retrieve documents based on query images which can help the police to establish the identity of criminals. The average precision achieved by the new scheme is 97.66 which indicated an excellent ability to identify wanted persons (criminals) and to retrieve the right documents. The most important features of the proposed scheme are: (1) use of the authentication phase to ensure only the right PO can access the image retrieval system (2) use of encapsulation and decapsulation of secret key (3) all images are encrypted before saving in a database, which means that this proposed scheme is able to resist malicious attacks such as spyware or the man in the middle (4) creation time of a database is minimized, and (5) short retrieval time of query images. For future work, the researchers intend to run the proposed scheme online in real time.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

- Ahmad, J., Muhammad, K., Bakshi, S., & Baik, S. W. (2018). Object-oriented convolutional features for fine-grained image retrieval in large surveillance datasets. *Future Generation Computer Systems*, 81, 314–330.
- Bartoli, A., Hernández-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., & Barthel, D. (2011, December). Security and privacy in your smart city. In *Proceedings of the Barcelona Smart Cities Congress* (Vol. 292, pp. 1–6).
- Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 1392–1393.
- da Silva Torres, R., & Falcao, A. X. (2006). Content-based image retrieval: Theory and applications. *RITA*, 13(2), 161–185.

- Dixit, U. D., & Shirdhonkar, M. S. (2017). Face Biometric-Based Document Image Retrieval Using SVD Features. In *Computational Intelligence in Data Mining* (pp. 481–488). Springer.
- Dixit, U. D., & Shirdhonkar, M. S. (2018). Face-based Document Image Retrieval System. *Procedia Computer Science*, 132, 659–668.
- Dr. Libor Spacek, Faces Directories, Faces 94 Directory, <http://cswww.essex.ac.uk/mv/allfaces>
- Du, A., Wang, L., Cheng, S., & Ao, N. (2020). A Privacy-Protected Image Retrieval Scheme for Fast and Secure Image Search. *Symmetry*, 12(2), 282.
- Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., & Al-Fuqaha, A. (2017). Smart cities: A survey on data management, security, and enabling technologies. *IEEE Communications Surveys & Tutorials*, 19(4), 2456–2501.
- Gracia, T. J. H., & García, A. C. (2018). Sustainable Smart Cities. Creating Spaces for Technological, Social and Business Development. *Boletín Científico de Las Ciencias Económico Administrativas Del ICEA*, 6(12).
- Haddadnia, J., Faez, K., & Ahmadi, M. (2003). A fuzzy hybrid learning algorithm for radial basis function neural network with application in human face recognition. *Pattern Recognition*, 36(5), 1187–1202.
- Haralick, R. M., Shanmugam, K., & Dinstein, I. H. (1973). Textural features for image classification. *IEEE Transactions on Systems, Man, and Cybernetics*, 6, 610–621.
- Huang, F., Jin, C., Zhang, Y., Weng, K., Zhang, T., & Fan, W. (2018). Sketch-based image retrieval with deep visual semantic descriptor. *Pattern Recognition*, 76, 537–548.
- Kumar, S. A., Vealey, T., & Srivastava, H. (2016). Security in Internet of Things: Challenges, solutions and future directions. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 5772–5781.
- Li, Y., Zhang, Y., Huang, X., Zhu, H., & Ma, J. (2018). Large-scale remote sensing image retrieval by deep hashing neural networks. *IEEE Transactions on Geoscience and Remote Sensing*, 56(2), 950–965.
- Liliana, D. Y., Basaruddin, T., Widyanto, M. R., & Oriza, I. I. D. (2020). High-level fuzzy linguistic features of facial components in human emotion recognition. *Journal of Information and Communication Technology*, 19(1), 103–129.
- Makrushin, D., & Dashchenko, V. (2016). Fooling the smart city. *Technical Report*, 1–22.
- Martínez-Ballesté, A., Pérez-Martínez, P. A., & Solanas, A. (2013). The pursuit of citizens' privacy: A privacy-aware smart city is possible. *IEEE Communications Magazine*, 51(6), 136–141.

- McLaren, D., & Agyeman, J. (2015). *Sharing cities: A case for truly smart and sustainable cities*. MIT press.
- Meng, X., An, Y., He, J., Zhuo, Z., Wu, H., & Gao, X. (2016). Similar image retrieval only using one image. *Optik*, 127(1), 141–144.
- Musa, S. *Smart City Roadmap* [Electronic resource] / S. Musa // Academia. – 2016. – Available at: \www/URL: [http:// www.academia.edu/21181336/Smart_City_Roadmap](http://www.academia.edu/21181336/Smart_City_Roadmap)
- Qin, H., Li, H., & Zhao, X. (2010). Development status of domestic and foreign smart city. *Global Presence*, 9, 50–52.
- Wang, X., Duan, X., & Bai, X. (2016). Deep sketch feature for cross-domain image retrieval. *Neurocomputing*, 207, 387–397.
- Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal*, 1(1), 22–32.