Offline Recognition of Handwritten Signatures Based on the SURF and SVM Algorithms

Hossam E. Abd El Munim, Ali Khaleel Ibrahim Hamadly and Hoda K. Mohamed
Department of Computer and Systems Engineering, Faculty of Engineering,
Ain Shams University, Cairo, Egypt

Abstract: Signature biometric becomes one of most relevant security factors in modern ubiquitous applications. Signature recognition is the process of using this biometric to verifying and identifying people accurately. There are several challenges associated with reliable recognition of these signatures. In this study, we have proposed a new approach for offline signature recognition. The SURF algorithm is used in this approach to specify invariant key points and descriptors while SVM algorithm is used for classification purposes. In addition, BOW algorithm is used to build dictionary of the most discriminative features of the handwritten signatures. Feature extraction and recognition are the key elements in the proposed approach for offline signature recognition. Our approach outperforms compared state-of-art approaches by providing 98.75% signature recognition accuracy.

Key words: SURF, SVM, feature extraction and BOW, descriptors, dictionary, recognition

INTRODUCTION

Biometrics are the psychological and behavioural characteristics of the human beings. Biometrics traits may be face, iris, fingerprint, voice or signature (Abboud and Jassim, 2012). They can be used in various important applications to provide services like authentication and identification of persons (Abboud and Jassim, 2010). Also, these biometric traits have special properties that characterize them from other authentication techniques such as passwords or tokens (Sae-Bae and Memon, 2014; Abaza *et al.*, 2013). These properties that they cannot forget or stole easily and also can be combined with other kinds of authentication technologies easily to provide more secure systems (Abboud and Jassim, 2012). The biometric authentication systems can be categorized according to the way of how biometric trait is used (Al-Assam *et al.*, 2011a, b). Hence, there are two categories in this classification which are offline and online systems (Abboud *et al.*, 2009). For instance, the offline signature authentication systems are depending on the acquisition of close image of the person signature while the online counterpart is depending on the distance acquisition of the signature image (Plamondon and Srihari, 2000; Shamir and Tauman, 2001). Handwritten signatures are behavioural traits of the human being. They have powerful features such speed, pressure and writing direction of signing that make them best candidate in the government and special agencies for person authentication (Al-Assam *et al.*, 2011a, b; Gruber *et al.*, 2010; Jassim *et al.*, 2010; Al-Assam *et al.*, 2012). We can classify the signature recognition algorithms into global and the local feature. The local feature category is always wider than the global counterpart but still there are some connections between them. Examples on the applications of those two categories are video information building senses, robot restriction surface confession and object section recognition (Richiardi *et al.*, 2005; Abboud, 2011). For example, we can use online signature verification based on local Fourier descriptors and pre-processing step is multi sub-step before feature extraction which includes the time normalization and stroke concatenation. Another example, it uses global features extracted using a number of categorizers and also they use multi-matcher for the online signature verification. In addition, the pre-processing step in this research is profoundly reliant on hashing threshold. Some researchers also suggest an online mark confirmation and acknowledgment framework that is based on taking the signatures symbolic representation by investigate the global features. Additionally, they have given the idea of compose subordinate limit and highlight subordinate edge prompting beat other worldwide element-based systems by multifactor ingredients (Impedovo *et al.*, 2012;

Corresponding Author: Hossam E. Abd El Munim, Department of Computer and Systems Engineering, Faculty of Engineering, Ain Shams University, Cairo, Egypt

Abboud, 2015a, b). Furthermore, there is another research direction that utilized three nearby highlights in respect to the main purpose of mark direction, the x and y arrange contrasts between two back to back focuses and the ebb and flow contrasts between two successive focuses (Parodi *et al.*, 2012; Abboud and Saleh, 2014).

Lastly, one research study proposed an offline method for signature acknowledgment by utilizing SURF highlight extraction and neural systems (Kaur and Kaur, 2014; Abboud *et al.*, 2018). Finally, we have to add that the security of biometric templates in the database (i.e., signature templates) and the communication channel is very important for online signature verification and recognition systems (Abboud, 2015a, b). Hence, the best way is to use encryption technologies to secure templates and communication channels over computer networks and use efficient routing and scheduling algorithms (Albu-Rghaif *et al.*, 2018; Farhan *et al.*, 2018).

MATERIALS AND METHODS

Universal signature dataset: In our experiments, we have used universal English signature dataset to prove the viability of our approach to recognize and verify signatures. This standard dataset has been selected from German web site that includes 240 images for 10 persons. This means that there are 24 signatures images per each person submitted to the system. The images of each person are classified into two sets. The first set consists of 16 signature images for learning while there are 8 signature images in the second set for testing. The number of signatures used for learning is about 116 that will be sent via. sequence of algorithms until it grouped into 10 classes (Liwicki *et al.*, 2011). The remaining number of signatures is eighty signatures will be sent for the testing as shown in Fig. 1.

This manipulation was in the form of adding different kinds of noises to the signature images. The images of this portions were manipulated at different levels of noise and based on this principle are classified into low noise signature images as shown in Fig. 2.

The second signature dataset which has used consist of 2064 signatures images classified into1360 images for learning and 680 images for testing purpose. Portion this dataset was created by manipulating the images by using three different printers. This manipulation was in the form of adding different kinds of noises to the signature images. The images of this portions were manipulated at different levels of noise and based on this principle are classified into low, medium and high noise signature images like the image shown in Fig. 2.
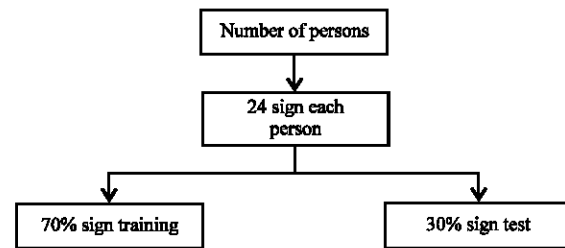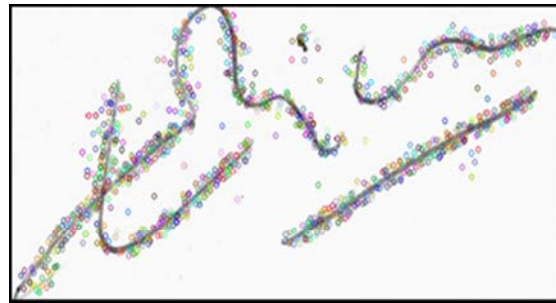

Fig. 1: Signature dataset division

Fig. 2: Signature images with different levels of noise

Proposed signature recognition system: We proposed in this research an offline recognition system of human handwritten signatures. Several components constitute the proposed system including database, signature recognition and prediction. The proposed system works in two phases which are training and testing. The training phase is used to train the system with user's signature discriminative features while testing phase is used to verify or recognize the user signature feature submitted by user. Speed up Robust Feature algorithm (SURF) is used to extract signature features and descriptor and the key points. Then these features are submitted to the Bag of Word algorithm (BOW) in aim to build dictionary of user's signatures. Support Vector Machine algorithm (SVM) is employed with different kinds of Kernels as a classifier. The testing phase uses SVM Model and other modules to create and implement jobs to recognize and predict tested images submitted by the client. The Oracle database includes all the necessary data for prediction. Figure 3 shows the proposed system in sufficient details and describes the basic components of the system. In the following, we explain these basic components in more details as follows.

Signature upload: The first component in the proposed system is responsible on uploading the signature image. The image of the signature is then transferred to the signature recognition component as shown in Fig. 3. In
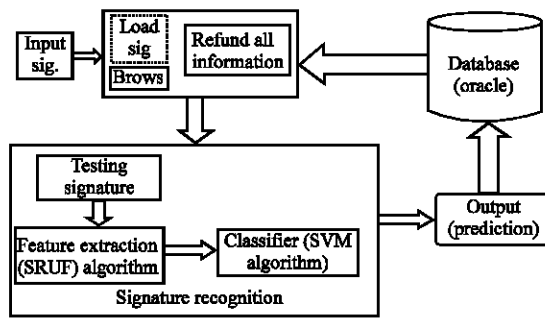
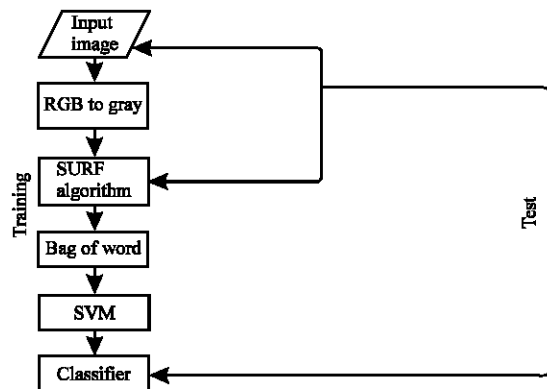Fig. 3: Offline signature recognition system

Fig. 4: Signature recognition process

the signature recognition process, the system uses the SURF algorithm to identifying the key point and interpreter in the extraction of features and also identifying the signature by matching with the previous workbook with which we conducted the training process. At this point, ID is retrieved from the prediction (output).

Signature recognition: This component in the proposed system is one of the most important stages where the process of prediction is occurred. The input to the proposed system is the image of person signature that we want to recognize. The output of the proposed system is the recognition or verification of an object or a group of objects appearing in the input signature image. The proposed framework comprises of several processes as shown in Fig. 4. The first process is the pre-processing of the input signature image by changing it from color space to grayscale space. The next process is the feature extraction using SURF algorithm and training dictionary using these features for future use. The final process is the classification of signature image using SVM algorithm. More details on the proposed system in the following sub-sections.

Preprocessing and feature extraction: The input signature image is pre-processed by converting it from

Fig. 5: Example of integral image

RGB format into gray format. Then, we will use SURF and BOW algorithms for feature extraction and training. These two algorithms are explained thoroughly in the following sub-sections.

SURF algorithm: The SURF algorithm is used to create object features. It depends on two needs that are holistic as shown in Fig. 5. Key point: points that mark existence of feature or are points and of the features in the form of numbers calculated by computation of integral image. The purpose of integral image is to establish fast filtering of box which was initially presented in vision of computer by Viola and Jones (2004). In the image integral step related to accumulative intensity of pixel added from places left and above an aimed pixel in the picture. The image of integral at index (x, y) is verified as:

$$jj(a \times b) = \sum_{d \leq a,\, b \leq b} j(a \times b) \qquad (1)$$

where, $j(a, b)$ indicate the pixels intensity placed at all locations achieved the not similarities $a<a$ and $b<b$ (Viola and Jones, 2004). As displayed in Fig. 5, the image of integral can be calculated on the input image quickly by accumulative adding initially all rows of a density of image, next all columns.

Speed up robust feature algorithm is depend on multiple scale theory of space and the detector of feature is depending on matrix of Hessian. Ever after matrix of Hessian has good behavior and precision. The matrix of Hessian H(f) is verified as the second degree matrix of square of partial derivatives of a function f(x, y) as supposed by McTear *et al.* (2016). In picture I, x = (x, y) is the given point and 3-Descriptor the translator (angle, lighting, edge, rotation, etc.). The main reasons that motivated us to utilize SURF algorithm are can choose the signature in any shape do not require to calculate size again do not require overall operations before process again that direct to system accelerate.

BOW algorithm: This algorithm is used to build a wordbook (or dictionary) of signature features. The built dictionary excludes certain vocabulary such words or numbers that available in descriptor (do not repeat same words or features). It utilizes the submitted powerful
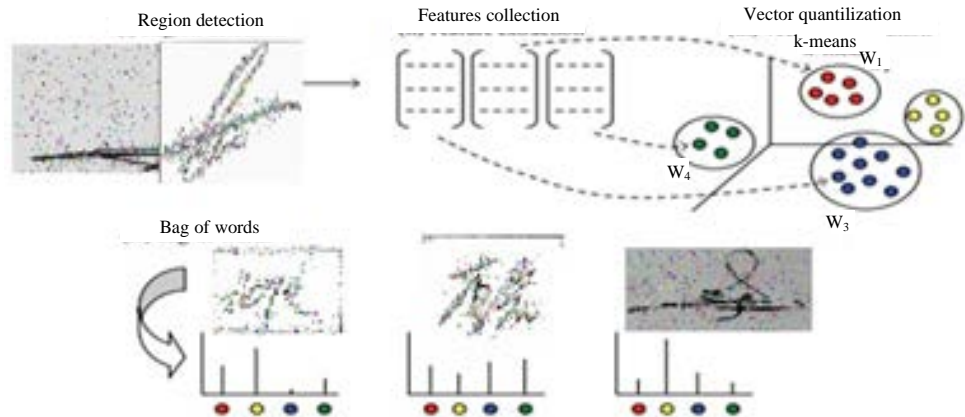
Fig. 6: Four construction steps using k-mean in the BOW algorithm

features to the system and neglecting features that have weak recurrence because it is not essential in beginning of strongest features or recurrence. The bag of word based on:

k-mean: Determine the appearance in the picture of every particular word in the dictionary for creating the bag of word feature (or word frequencies histogram) (McTear *et al.*, 2016). Figure 6 explain these four stages to exclude the bag of word feature from pictures. The bag of word model can be verified as follows. Given a dataset of training (S) including (m) pictures depicted by S = s1, s2, ... and sn where, s is the excluded visual features, a particular not supervised algorithm of learning, like as k-means is applied to group S depend on a constant number of visual words X (or kinds) depicted by $X = x_1, x_2,$ ... and x_v where, Y is the number of cluster. Then, we can abstract the data in a Y×N co-occurrence counts table $N_{ij} = N_{ij} (x_i, s_j)$ where, m (x_i, s_j) indicates how occasionally the word x_i happen in a picture s_j.

F-kNN (Fast Approximate Nearest Neighbor): Working of k-NN is demonstrated in Fig. 7 where, N training vectors are given and k-NN algorithm identifies the k-nearest neighbor of 'c'. Feature 'c' needs to be classified either in class 'a' or class 'o'. For instance, the value of k is taken 3. So, k-NN algorithm looks for 3 nearest neighbor for feature 'c'. And it turns out two features of class 'o' and one feature of class 'a' resides in the very vicinity of 'c'. Since, class 'o' has outvoted class 'a', feature 'c' is declared to have belonging with class 'o'. Selection of K's value is critical. The value of 'K' is chosen in such a way that it is always odd and is not the multiple of the number of classes to avoid the ties
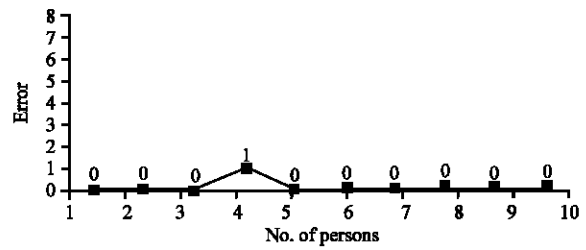

Fig. 7: Error curves vs. number of persons

(Ali *et al.*, 2016; Cheng *et al.*, 2015). The advantages of bag of word are assorting features in dictionary form to be simple deal with it also show powerful features and at last quicken the system.

Classification: After feature extraction of signature images using SURF and BOW algorithms, SVM algorithm is used for signature image classification. The data involvement descriptor for training to be isolated and classified into ten classes by using classifier with various kernels. Every class carries specific identification from ID1 until Idx. The linear, non-linear, poly (D = 1) and poly (D = 2) are the kernels used with SVM classifier. The narrow lines in Fig. 8 in case b are rims or side. The wide line in the medium is named the limit of band. The nodes which place on the sides are the support vectors. The split hyper plane is as distant as allowable from the points of sample. The support vectors are the nearest to the optimal hyper plane. Suitable element fittings in the kernels increment support vector machine accuracy of classification. There are two elements to be considered in the model of SVM with the kernel of RBF: B and gamma (γ). The gamma element dynamically verifies the space which a unique example of training can arrive with small
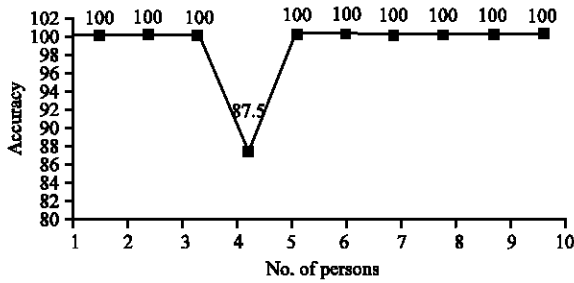
Fig. 8: Non-linear RBF and linear accuracy

Fig. 9: Percentage of different techniques used

values indicate 'distant' and big values indicate 'near. The B element provides the training examples trade off wrong classification contrast simplicity of decision surface. Smaller B values guarantee a flat surface of decision while bigger B values try to determine accurate training examples. Carried out experiments perform to estimate performance of SVM via. changes of the gamma and B elements.

Database (search part): ID is sent to the database where there are tables for all information about each ID such as name, father's name, mother's name, workplace, blood category. Bring any ID to Oracle) matches the information in which it is stored to identify the person who is signed.

Prediction: Following SVM operation, inspect and test operation began by accepting the left eight signatures for every person (i.e., 80 signatures in total for all persons). The former processes are utilizing the similar algorithms such as SURF. Then, it will be sent to the classifier to detect the identification and coincidence to any person. The testing and training operations achieved good prediction accuracy.

RESULTS AND DISCUSSION

We have conducted experiments to prove the viability of our proposed system to recognize robustly the signatures of persons. Two standard signature datasets were used in our experiments to test our system on a wide range of different signatures. The first dataset contains 240 signs of 10 persons. From the results of this dataset in Table 1, we can found that the SVM classifier with (Poly = 1) gave best classification accuracy (100%) among other kernels. However, the other kernels gave the following accuracies sequentially: (Precision linear+RBF) = No hit/No test = 79/80 = 98.75) the, nonlinear Radial Base Function (RBF) shows an accuracy of (98.75%), linear shows (98.75%) and Poly = 2 provide us with (77.5%) accuracy. Figure 7 shows the error in regard to the
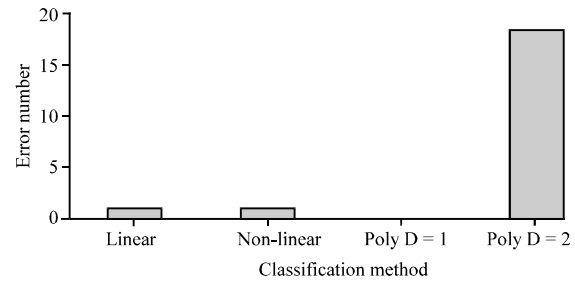
Table 1: Comparsion of signature classification accuracy using different kernels of SVM classifier for first tested dataset

Technique	Accuracy (%)	Comments
Non-linear (RBF)	98.75	Precision = No hit/No test = 79/80 = 98.75
Linear	98.75	Precision = No hit/No test = 79/80 = 98.75
Poly = 1	100	Precision = No hit/No test = 80/80 = 100
Poly = 2	77.5	Precision = No hit/No test = 62/80 = 77.5

Table 2: Table of eerors number and accuracy for each person

No. of persons	Errors number	Comments	Accuracy (%)
[1[h1]], 2, 3, 5, 6, 7, 8, 9, 10]	0	No hit/No test = 8/8 = 1*100	100
[4]	1	No hit/No test = 7/8 = 0.875*100	87.5

number of persons. From this SVM classifier, we can analyze the error as shown in Fig. 7. We can notice from Fig. 7 that the number of errors is minimal for all persons and it is zero for nine persons. However, this error is one for person number four.

Figure 8 shows that the accuracy of the system for each person is 100% except person four is 87.5%. These results provide another evidence that our proposed system is robust enough to recognize the signatures of persons. Table 2 shows the errors number per each person individually while Table 3 shows the errors number for all persons together (i.e., whole recognition system). Table 4 is presented to compare the proposed signature recognition system with state of art approaches. Two approaches have been compared with the proposed system and the comparison results are shown in Table 4. One of these resaerchers used combined method with Hough transform as classifier and they got a recognition of 94.60 (Oloyede and Hancke, 2016). Another researcher used back propagation Neural Network (NN) as classifier and they got a recognition of 82.60 (Pansare and Bhatia, 2012). The recognition phase in our proposed system as follows: SURF (SVM-RBF) with recognition 98.75%. From these experimental results, we can notice that our proposed signature recognition system outperforms other approaches. Figure 9 represent the accuracy of all

Table 3: Table of eerors number and accuracy for all persons

No. of persons	Errors number	No. of tested images	Comments	Accuracy
10	1	80	No hit/No test = 79/80 = 0.9875*100	98.75%

Table 4:Comparison of the proposed system with other systems

Researchers	Classifiers	Recognition rate (%)
Porwik *et al.*	Combined method with Hough transformation	94.60
Pansare and Bhatia (2012)	Back propagation NN	82.60
The proposed system	SURF (SVM-RBF)	98.75

Table 5: Error number and accuracy of each person

No. of persons	Errors numbers	Comments	Accuracy (%)
[1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16, 17, 19, 20, 21, 22, 23, 24, 27, 28, 30, 31, 32]	0	No. hit/No. test = 8/8 = 1*100	100
[4, 14, 18, 25, 26, 29, 35, 39, 45, 48, 55, 56, 67, 77, 78, 79, 81, 83, 85]	1	No. hit/No. test = 7/8 = 0.875	87.5

Table 6: Error number and accuracy for the whole system

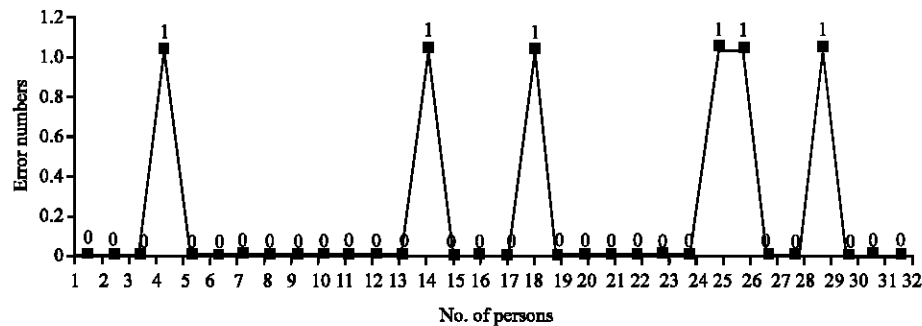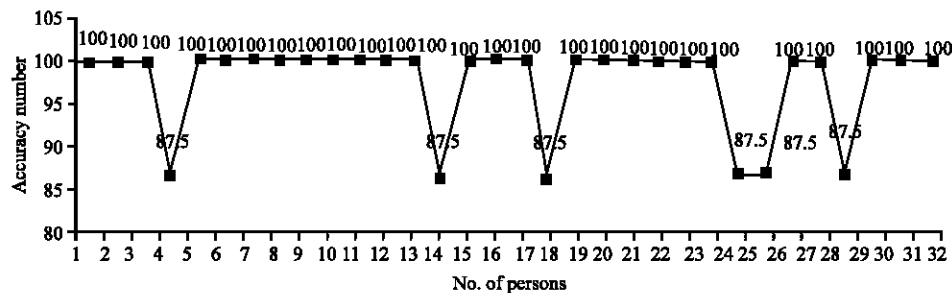| No. of persons	Errors number	No. of image testing	Comments	Accuracy (%)
32	6	256	No hit/No test = 250/256 = 0.977*100	97.7

Fig. 10: Error curve

Fig. 11: Accuracy curve

techniques used in this research as follows for the first signature dataset. We have also conducted a second group of experiments on the second signature dataset using SVM classification method with linear and non-linear kernels and their results as follow. From Table 5 and 6, respectively shows the accuracy for each person and system. It can be drawing the curve for error and accuracy for each person as shown in Fig. 10 and 11. From Table 6, it can be obtained of the second datasets the following curve as shown in Fig. 12.
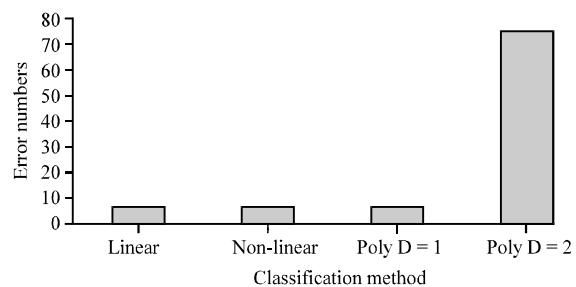

Fig. 12: Percentage of different techniques used

CONCLUSION

We have proposed in this study an offline signature recognition system. This signature recognition has used SURF and BOW algorithms and also SVM classifier. In this system, we can load any signature and examined through the processes of recognition and verification and refund the data in high velocity and accuracy. We obtained approximately 98.75% classification accuracy for the first and second used standard datasets. The main characteristics of the proposed system are we obtained good results in terms of recognition accuracy using oracle data base to refund the data base to a server because they have high security and quick to deal with Java.

REFERENCES

Abaza, A., A. Ross, C. Hebert, M.A.F. Harrison and M.S. Nixon, 2013. A survey on ear biometrics. ACM. Comput. Surv., 45: 1-35.

Abboud, A.J. and O.S. Saleh, 2014. Sustainable IT: A realisation survey among academic institutions of Ira. Intl. J. Enhanced Res. Sci. Technol. Eng., 3: 25-31.

Abboud, A.J. and S.A. Jassim, 2010. Image quality guided approach for adaptive modelling of biometric intra-class variations. Proceedings of the SPIE Conference on Mobile Multimedia/Image Processing, Security and Applications Vol. 7708, April 28, 2010, SPIE, Orlando, Florida, USA., pp: 1-10.

Abboud, A.J. and S.A. Jassim, 2012. Biometric Templates Selection and Update using Quality Measures. In: Mobile Multimedia/Image Processing, Security and Applications 2012, Agaian, S.S., S.A. Jassim and E.Y. Du (Eds.). SPIE Press, Bellingham, Washington, USA., ISBN: 9780819490841, pp: 1-9.

Abboud, A.J., 2011. Quality aware adaptive biometric systems. Ph.D Thesis, University of Buckingham, Buckingham, England.

Abboud, A.J., 2015b. Multifactor authentication for software protection. Diyala J. Eng. Sci., 8: 479-492.

Abboud, A.J., 2015a. Protecting documents using visual cryptography. Intl. J. Eng. Res. General Sci., 3: 464-470.

Abboud, A.J., A.N. Albu-Rghaif and A.K. Jassim, 2018. Balancing compression and encryption of satellite imagery. Intl. J. Electr. Comput. Eng., 8: 3568-3586.

Abboud, A.J., H. Sellahewa and S.A. Jassim, 2009. Quality Based Approach for Adaptive Face Recognition. In: Mobile Multimedia/Image Processing, Security and Applications 2009, Agaian, S.S. and S.A. Jassim (Eds.). SPIE Press, ?Bellingham, Washington, USA., ISBN: 9780819476173, pp: 1-10.

Al-Assam H., A. Abboud, H. Sellahewa and S. Jassim, 2012. Exploiting Relative Entropy and Quality Analysis in Cumulative Partial Biometric Fusion. In: Transactions on Data Hiding and Multimedia Security VIII, Shi, Y.Q. and S. Katzenbeisser (Eds.). Springer, Berlin, Germany, ISBN:978-3--642-31971-6, pp: 1-18.

Al-Assam, H., A. Abboud and S. Jassim, 2011b. Exploiting samples quality in evaluating and improving performance of biometric systems. Intl. J. Digital Soc., 2: 462-468.

Al-Assam, H., A. Abboud and S. Jassim, 2011a. Hidden assumption of face recognition evaluation under different quality conditions. Proceedings of the 2011 International Conference on Information Society (i-Society), June 27-29, 2011, IEEE, London, UK., ISBN:978-1-61284-148-9, pp: 27-32.

Albu-Rghaif, A.N., A.K. Jassim and A.J. Abboud, 2018. A data structure encryption algorithm based on circular queue to enhance data security. Proceedings of the 2018 Joint 1st and 3rd International Scientific and Engineering Sciences Scientific Conference on Engineering Science (ISCES), January 10-11, 2018, IEEE, Diyala, Iraq, ISBN:978-1-5386-1498-3, pp: 24-29.

Ali, N.M., S.W. Jun, M.S. Karis, M.M. Ghazaly and M.S.M. Aras, 2016. Object classification and recognition using Bag-of-Words (BoW) Model. Proceedings of the IEEE 12th International Colloquium on Signal Processing and its Applications (CSPA), March 4-6, 2016, IEEE, Malacca, Malaysia, ISBN:978-1-4673-8781-1, pp: 216-220.

Cheng, G., Y. Wan, A.N. Saudagar, K. Namuduri and B.P. Buckles, 2015. Advances in human action recognition: A survey. Prepr., 1: 1-30.

Farhan, L., L. Alzubaidi, M. Abdulsalam, A.J. Abboud and M. Hammoudeh *et al.*, 2018. An efficient data packet scheduling scheme for Internet of Things networks. Proceedings of the 2018 1st and 3rd International Scientific Conference on Engineering Sciences (ISCES), January 10-11, 2018, IEEE, Diyala, Iraq, ISBN:978-1-5386-1499-0, pp: 1-6.

Gruber, C., T. Gruber, S. Krinninger and B. Sick, 2010. Online signature verification with support vector machines based on LCSS kernel functions. IEEE. Trans. Syst. Man Cybern. Part B. Cybern., 40: 1088-1100.

Impedovo, D., G. Pirlo and R. Plamondon, 2012. Handwritten signature verification: New advancements and open issues. Proceedings of the International Conference on Frontiers in Handwriting Recognition, September 18-20, 2012, IEEE, Bari, Italy, ISBN:978-1-4673-2262-1, pp: 367-372.

Jassim, A.J., H. Al-Assam, A.J. Abbound and H. Sellahewa, 2010. Analysis of relative entropy, accuracy and quality of face biometric. Proceedings of the Workshop on Pattern Recognition for IT, September 21, 2010, DAGM, Stuttgart, Germany, pp: 1-8.

Kaur, H. and S. Kaur, 2014. Offline Hindi signature recognition using surf feature extraction and neural networks approach. Intl. J. Sci. Res., 3: 1141-1146.

Liwicki, M., M.I. Malik, C.E.V.D. Heuvel, X. Chen and C. Berger *et al.*, 2011. Signature verification competition for online and offline skilled forgeries (SigComp2011). Proceedings of the International Conference on Document Analysis and Recognition, September 18-21, 2011, IEEE, Beijing, China, ISBN:978-1-4577-1350-7, pp: 1480-1484.

McTear, M., Z. Callejas and D. Griol, 2016. The Conversational Interface: Talking to Smart Devices. Springer, Berlin, Germany, ISBN:9783319329659, Pages: 422.

Oloyede, M.O. and G.P. Hancke, 2016. Unimodal and multimodal biometric sensing systems: A review. IEEE. Access., 4: 7532-7555.

Pansare, A. and S. Bhatia, 2012. Article: Handwritten signature verification using neural network. Int. J. Applied Inf. Syst., 1: 44-49.

Parodi, M., J.C. Gomez and M. Liwicki, 2012. Online signature verification based on Legendre series representation: Robustness assessment of different feature combinations. Proceedings of the International Conference on Frontiers in Handwriting Recognition, September 18-20, 2012, IEEE, Bari, Italy, ISBN:978-1-4673-2262-1, pp: 379-384.

Plamondon, R. and S.N. Srihari, 2000. On-line and off-line handwriting recognition: A comprehensive survey. 1EEE Trans. Pattern Anal. Mach., 22: 63-84.

Richiardi, J., H. Ketabdar and A. Drygajlo, 2005. Local and global feature selection for on-line signature verification. Proceedings of the 8th International Conference on Document Analysis and Recognition (ICDAR'05), August 31-September 1, 2005, IEEE, Seoul, South Korea, ISBN:0-7695-2420-6, pp: 625-629.

Sae-Bae, N. and N. Memon, 2014. Online signature verification on mobile devices. IEEE. Trans. Inf. Forensics Secur., 9: 933-947.

Shamir, A. and Y. Tauman, 2001. Improved Online/Offline Signature Schemes. In: Advances in Cryptology-CRYPTO 2001, Kilian, J. (Ed.). Springer, Berlin, Germany, ISBN:978-3-540-42456-7, pp: 355-367.

Viola, P. and M.J. Jones, 2004. Robust real-time face detection. Int. J. Comput. Vision, 57: 137-154.