A Digital Signature System Based on Real Time Face Recognition

Conference Paper · October 2019

DOI: 10.1109/ICSEngT.2019.8906410

5 authors, including:

Taha Hasan
University of Diyala
58 PUBLICATIONS **197** CITATIONS
SEE PROFILE

Firas A. Abdullatif
University of Baghdad
26 PUBLICATIONS **74** CITATIONS
SEE PROFILE

Mustafa Sabah Taha
Missan Oil Trainining Institute (MOTI)
47 PUBLICATIONS **359** CITATIONS
SEE PROFILE

A Digital Signature System Based on Real Time Face Recognition

Asraa Ahmed
Department of computer science, College of Science, Diyala University
altamimiasra@gmail.com

Taha Hasan
Department of computer science, College of Science, Diyala University
dr.tahamh@sciences.uodiyala.iq

Firas A. Abdullatif
Universiet of Baghdad, College of Education for pure science-ibn AlHaitham,computer sceince department
Firas.alobaedy@gmail.com

Mustafa S. T.
School of Computing, Faculty of Engineering, University Technology Malaysia
Basrah Oil Traning Institute,Ministry of Oil , Iraq
timimymustafa@gmail.com

Mohd Shafry Mohd Rahim
School of Computing, Faculty of Engineering, University Technology Malaysia
shafry@utm.my

Abstract— **This study proposed a biometric-based digital signature scheme proposed for facial recognition. The scheme is designed and built to verify the person's identity during a registration process and retrieve their public and private keys stored in the database. The RSA algorithm has been used as asymmetric encryption method to encrypt hashes generated for digital documents. It uses the hash function (SHA-256) to generate digital signatures. In this study, local binary patterns histograms (LBPH) were used for facial recognition. The facial recognition method was evaluated on ORL faces retrieved from the database of Cambridge University. From the analysis, the LBPH algorithm achieved 97.5 % accuracy; the real-time testing was done on thirty subjects and it achieved 94 % recognition accuracy. A crypto-tool software was used to perform the randomness test on the proposed RSA and SHA256.**

Keywords— Digital signature, Face recognition, SHA256, RSA, LBPH

I. INTRODUCTION (*HEADING 1*)

One of the approaches to verify the authenticity of digital data transmitted between two parties is through digital signature. A digital signature is a mathematical system that guarantees the authenticity/originality of digital data. Through a valid digital data, the data recipient will verify that the data is coming from a known sender, thereby confirming the authenticity and non-repudiation of the data [1]. There are three stages in the digital signature system: key generation, message signing, and signature verification. The unique private and public keys are generated during the key generation stage. The generation of digital signatures requires an asymmetric encryption algorithm, in which the private key is accessible only to its owner while the public key is shared openly [2]. This paper proposed a new facial recognition technology-based digital signature scheme. In this new scheme, the user is meant to sign messages and documents using his/her face and each person's face serves as either a private or public key. For face recognition, the system uses local binary patterns histograms for features extraction and Euclidean distance to measure the distance between the facial feature vector of the image saved in the database and the image obtained from the camera. The system uses Rivest–Shamir–Adleman (RSA) asymmetric encryption algorithm for the generation of the digital signature, and a secure hash function (SHA256).

II. RELATED WORK

Several related methods to the proposed work in this study have been proposed in the literature. For instance, Hua Zhang et al. [8] proposed a two-party key agreement protocol by modifying the improved scheme as an extension of Chang-Chang's signature scheme. Thus, the proposed technique ensures the security in standard models by its capability to detect new forms of attack. However, it is not clear whether the protocol in the proposed technique remains secure in the presence of an adaptively selected attack. This issue will be addressed in future study. Wenbo et al. [9] proposed a digital signature and encrypting method based on a combined symmetric key and hardware technology. This technique avoids the problem of symmetric key management and a drastic speed increase. Similarly, the negative effect on office efficiency is minimized. Guifen et al. [10] presented a 3-layer structured scheme for digital documents. As per the authors, the system could be implemented easily with the available office automation systems. Documents management provides more convenience for users without space and time limitation. It can enhance users' work efficiency since it ensures security, storage, and distribution of the secret key. Turk et al. [11] proposed an eigenfaces approach for facial recognition. This approach is a popular facial recognition algorithm, which is based on principal components analysis (PCA). It allows the transformation of the training images into eigenfaces using dimensionality reduction. It is fast, relatively simple, and has been shown to work well in a somewhat constrained environment. Guo et al. [12] presented a face recognition system based on Support Vector Machines (SVM) with a binary tree recognition strategy for solving face recognition issues. The approach extracts features from faces before discriminating the face pairs learned by SVM. For face recognition, the experimental results showed that the SVM algorithm performs better than the nearest center approach . Magesh et al. [13] proposed a face recognition system based on Gabor features, LDA and neural network for classification. The performance evaluation of the system showed that the recognition rate for the selected database is

978-1-7281-0757-8

high with features extracted from LDA and PCA-based Gabor methods than simple PCA methods. The results also showed that increases in the number of features selected in PCA lead to the attainment of more discriminating features from LDA, thereby increasing the recognition rate. However, this increases the computational load. The authors in [14] studied energy minimization by implementing a dynamic scheduling framework to increase the mixing of hardware elements heterogeneity. The identification performance of this framework is significant. However, its cost and computational complexity are high. A neural spatiotemporal dynamics model for storing the database and matching stored faces with a face under observation has been developed by [15]. This model presented a good performance in real-time applications but suffers from a low level of reliability. Luo et. al. [16] presented a detection model using facial structure estimation. The model presented a high level of reliability, but complexity is high as well. The detection of faces far from the camera is difficult. Thus, the system requires improvements at several levels, i.e. preprocessing, feature estimations, and training [17].

III. RSA ENCRYPTION

The RSA cryptosystem is mainly used for securing sensitive data during its transmission over an insecure network. It is also known as asymmetric cryptography; it uses two different keys – a public key, which is accessible to everyone, and a private key, which is available only to the owner [3]. The schematic of the RSA algorithm is presented in the following figure.

IV. SHA (SECURE HASH ALGORITHM)

SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512). The SHA-2 family is more secure than their predecessors SHA- 1 family and MD5, due to the higher size of the hash. Additionally, SHA-512 is more secure but slower than SHA-256 . SHA-256 was chosen as a hash function when designing the proposed technique as it produces a fixed message length to be used in the digital signature [4].

V. LOCAL BINARY PATTERNS HISTOGRAM (LBPH)

The local binary pattern is a visual descriptor used in computer vision for task classification. It is an appropriate type of texture spectrum as proposed [5, 6]. With the LBP, feature vector is created by dividing the examined window into cells and comparing each pixel in these cells to its eight neighbours. If the value of the centre pixel is higher than the value of the neighbour, it will be recorded as ‘0’, ‘1’ otherwise.The histogram of the frequency of occurrence for each number over the cell is then computed as a 256-dimensional feature vector. Figure 1 shows the process of LBP. The LBP for face recognition uses the features of LBP code occurrences histogram for each image. The first step is to recognize faces using LBPH [7], then, the image is divided into local regions before extracting the LBP from each region. The histogram of each region is then concatenated to form the feature histogram of the given face. This process of facial description using LBP is depicted in Figure 2. The facial feature histogram can be described in three different locality levels: it has the information about the pixel-levels patterns; the LBP labels of the small regions are summed to produce the regional-level information. These local histograms are concatenated to build the face's feature histogram.

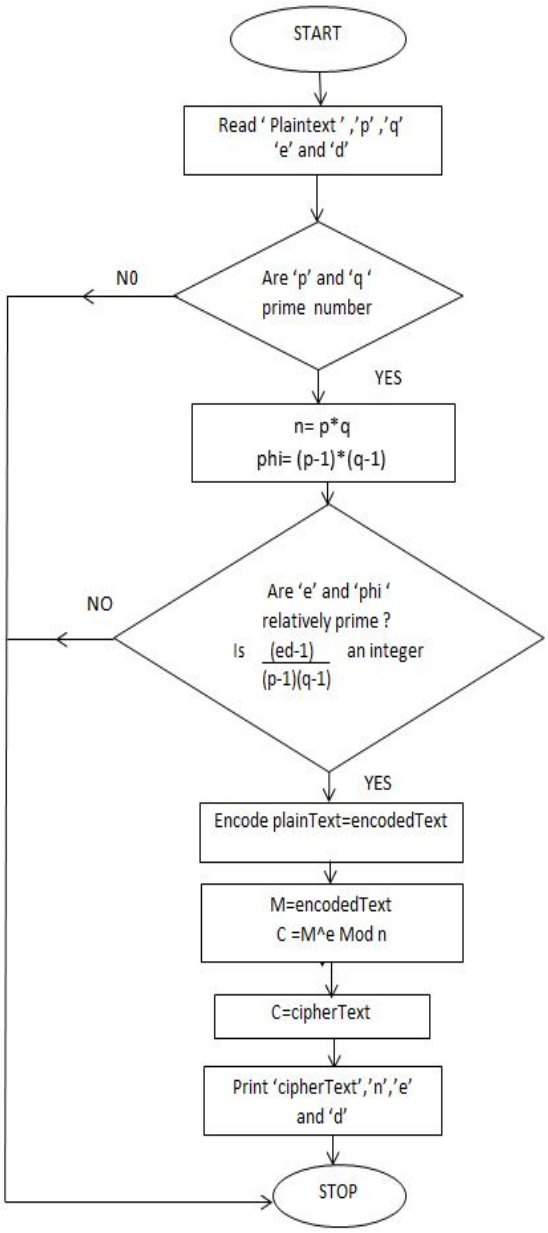

Fig 1. A flowchart illustrating the RSA algorithm

VI. PROPOSED METHOD

The proposed approach in this study uses biometric authentication such as facial recognition for account registration, login, and signing a digital document. This scheme provides a more secure and fast way of generating and transmitting digitally signed data over an insecure network. The proposed method in this paper uses the RSA

algorithm and SHA256 hash function to produce digitally signed messages. The flow chart of the system is presented in Figure 4.

The addition of a user to the system under the proposed approach requires admin login for security reasons. The person that manages the software must sign in to the software; then, will be asked to enter the prime numbers p and q to generate the public and private keys of the new person. After that, person's information, including the username and password are requested. The system is connected to the SQL database, which contains the keys and users' details. Upon the addition of a new user to the database, a gray-scale facial image of the user will be captured and added to the database to serve as the users' face feature vector. Figure 5 shows the flow chart of the main facial recognition-based digital signature program.

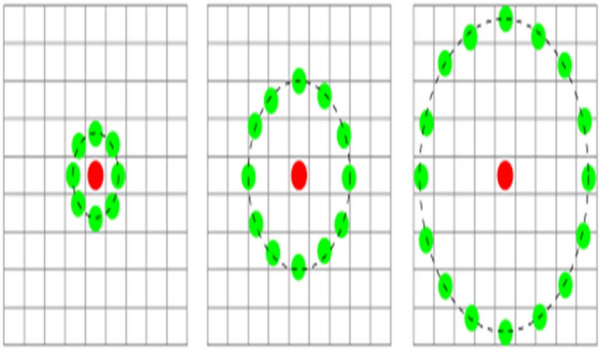

Fig 2. The Basic LBP process.

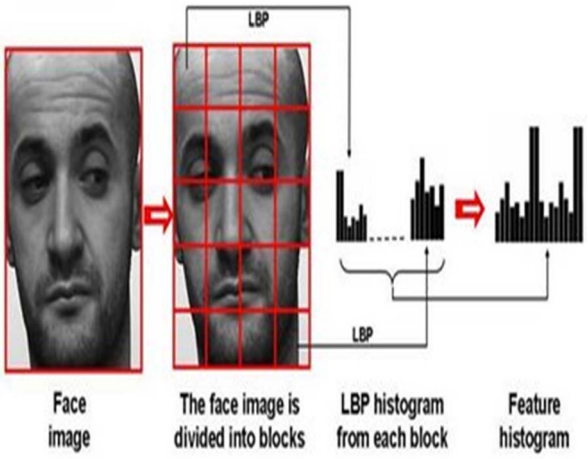

Fig 3. Facial description using LBP.

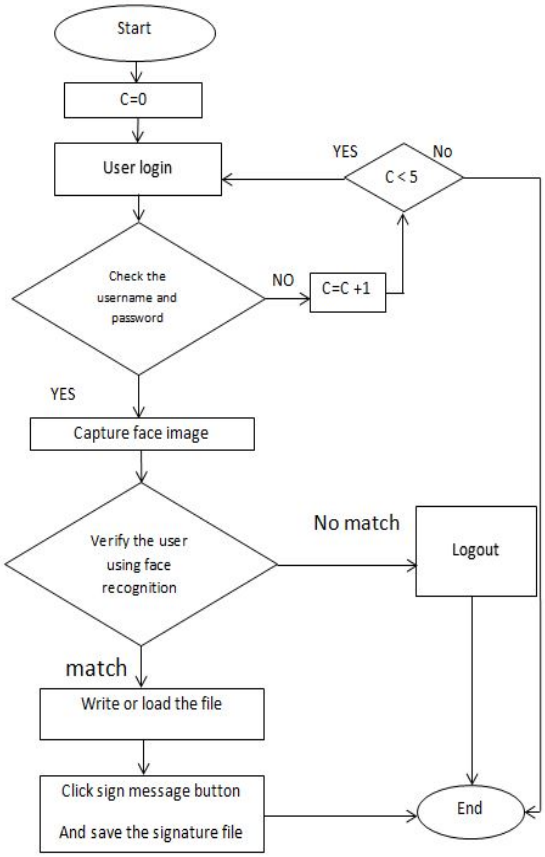

Fig 4. Adding a new person to the proposed digital signature system

VII. RESULTS AND EXPERMENTS

This paper proposed the use of the RSA and SHA256 algorithms for digital signature by using the biometric data system. The facial recognition aspect of the process is performed using local binary patterns histograms algorithm for features extraction while Euclidian distance was used to measure the similarity between feature vectors. The facial image of each user is extracted from the camera image using a HAAR cascade classifier. The system was validated on ORL faces dataset and it achieved 97.5 % accuracy. The real-time face recognition was validated on 30 subjects and it achieved 96 % accuracy.

.

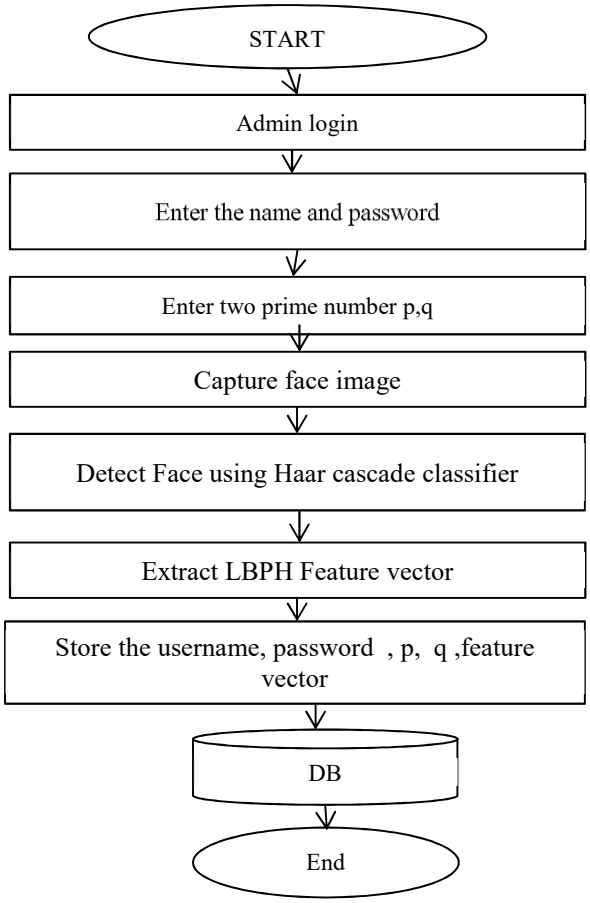

Fig 5. Work of the proposed system

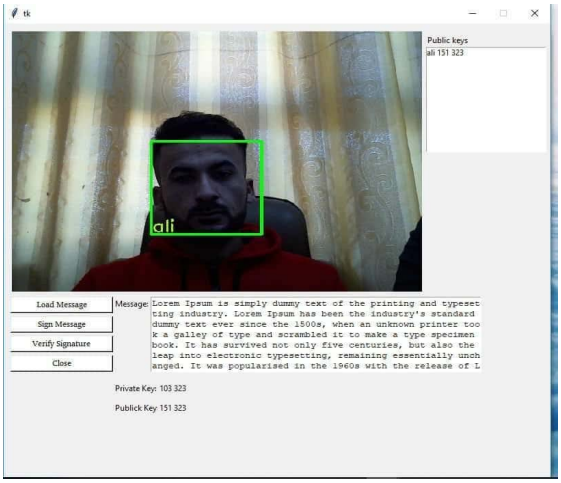

Fig 6. User login to the system software in real time

The random test performed on the encrypted file was presin the table below. The encryption was done by the RSA and SHA256. Randomness is an important standard in measuring and evaluating the strength and durability of encrypted files. To enhance the security and robustness of transmitters, a random sequence can improve the output of the encrypted file and identify the statistical weaknesses in the original text. Some tests for randomness are Frequency Test, Poker Test, Run Test, Long Run Test, and Serial Test. The result of Randomness tests in this study is shown in Table (1).Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as “3.5-inch disk drive”.

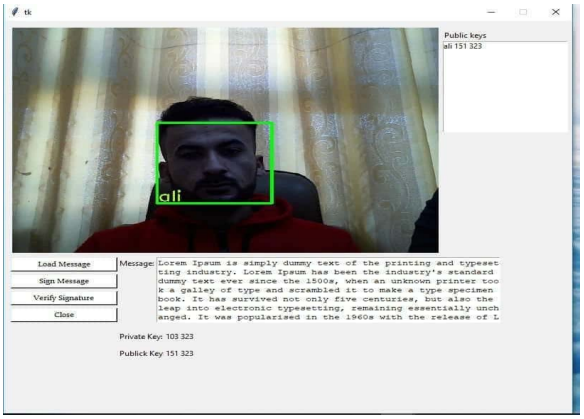

Fig 7. validation with the face and upload the document file in real time

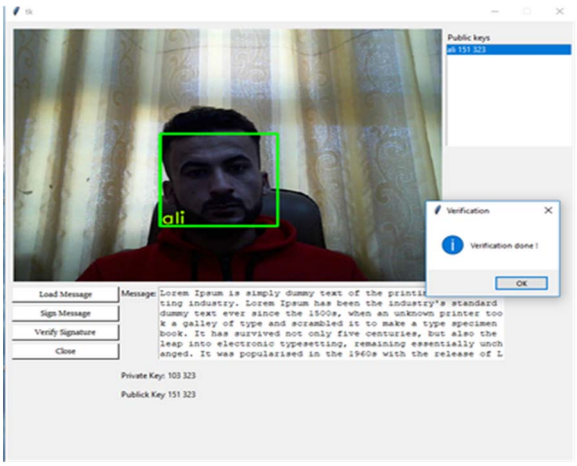

Fig 9. Verify that the signature process has completed in real time

VIII. CONCLUSION

This paper introduced a facial recognition-based digital signature scheme for the recognition of registered persons using face recognition and retrieving their private and public keys from the database using their features only. This approach eases the documents signing task. The cascaded RSA/SHA256 system was analysed and validated and the results show that the combined system has a better performance compared to the performance of its individual components. The proposed system also uses the LBPH algorithm for face recognition in real-time, where it has shown excellent performance as well. This paper highlighted the potential future study on the implementation

of facial recognition technology in documents signing and office automation systems.

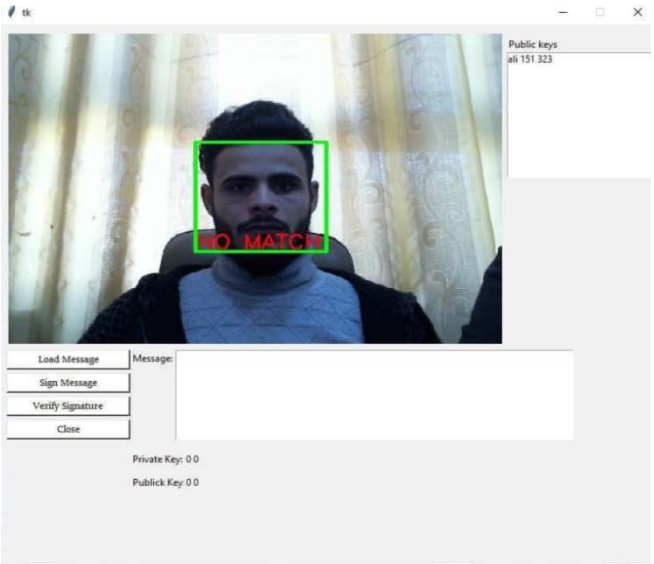

Fig 8. login a person who is not registered to the system in real time

TABLE 1. The Randomness test of RSA and SHA256 algorithms results.

NO OF TEST	File size .TXT	Frequency	Poker	Run test	Long run	Serial
		Test result/ Pass value(3.84)	Test result/ Pass value(14.7)	Test result/ Pass value(9.48)	Test result/ Pass value(34)	Test result/ Pass value(5.99)
1	1KB	0.11	5.39	8.1	6	3.3
2	2KB	0.08	8.25	9	8	4.49
3	4KB	0.96	9.08	13	6	4.75
4	5KB	0.05	6.15	11	9	4.52
5	9KB	0.32	6.48	12	6	3.65
6	14KB	0.02	13	6.8	6	0.2
7	21KB	0.19	11.78	6	8	0.06
8	23KB	3.44	11.4	13.44	6	4.4
9	29KB	1.47	9.03.	9	6	4
10	39KB	0.6	8.15	8	6	2.5
11	40KB	0.34	9.42	12	7	5.11
12	55KB	0.33	11.5	9	7	3.09
13	62KB	0.86	13.02	7	7	5.74
14	85KB	0.44	7	2.64	7	2.23
15	86KB	0.46	13.11	5	6	2.73
16	106KB	0.29	7.5	7.99	7	5.73
17	120KB	3.21	11.12	10	6	3.44
18	156KB	0.94	8.13	7	7	2.38
19	834 KB	1.93	13.45	9	6	3.53
20	1272KB	0.95	13.71	10	6	4.1

REFERENCES

[1] R. Rahim, A. Pranolo, and R. Hadi . " Digital Signature Security in Data Communication." Advances in Intelligent Systems Research (AISR). In: International Conference on Education and Technology (2017 ICEduTech),Vol 144 ,2017.

[2] Pooja, and Mrs. Mamta Yadav . " Digital Signature " International Journal of Scientific Research in Computer Science, Engineering and Information Technology. Vol.3 ,No. 6 , pp . 2456-3307 ,2018

[3] D. Kurnia, H. Dafitri , Sugianto, Mardiana and A. Siahaan." RSA 32-bit Implementation Technique." International Journal of Recent Trends in Engineering & Research (IJRTER). Vol.03,No.07,pp. 2455-1457,2017.

[4] Taha, Mustafa Sabah, et al. "Wireless body area network revisited." *International Journal of Engineering & Technology* 7.4 (2018): 3494-3504.

[5] D. He and L. Wang "Texture Unit, Texture Spectrum, And Texture Analysis," Geoscience and Remote Sensing, IEEE Transactions on, vol.28, pp. 509 - 512,(1990).

[6] L. Wang and DC. He "Texture Classification Using Texture Spectrum," Pattern Recognition, Vol. 23, No. 8, pp. 905 – 910 ,(1990).

[7] Ahonen, T., Hadid, A., and Pietikäinen, M, Face Description with Local Binary Patterns: Application to Face Recognition. IEEE Trans. Pattern Analysis and Machine Intelligence Vol.28,No.12,p.2037-2041, (2006).

[8] Zhang, Hua, Z. Yuan, and Q. Wen. "A digital signature schemes without using one-way hash and message redundancy and its application on the key agreement." Network and Parallel Computing Workshops. NPC Workshops. IFIP International Conference on. IEEE, 2007.

[9] Wu, Suyan, W. Li, and X. Hu. "Study of the digital signature with encryption based on the combined symmetric key." E-Business and Information System Security, 2009. EBISS'09. International Conference on. IEEE, 2009.

[10] Zhao, Guifen, et al. "Scheme for digital documents management in a networked environment." Network Infrastructure and Digital Content, 2009. IC-NIDC 2009. IEEE International Conference on. IEEE, 2009.

[11] Turk, A. Pentland, and A.P. "Face recognition using eigenfaces". In Proc of the IEEE Conference on Computer Vision and Pattern Recognition, Maui, HI, USA, Vol.3,No.6 ,pp. 586–591,1991.

[12] G. Guo, S. Z. Li, and K. Chan" Face recognition by support vector machines". In Proc of the IEEE International Conference on Automatic Face and Gesture Recognition, Grenoble, France, Vol.28,No.30, pp.196–201,2000.

[13] C. MageshKumar , R. Thiyagarajan , S. P.Natarajan , and S. Arulselvi . " Gabor features, and LDA based face recognition with ANN classifier". In Proc of the 2011 International Conference on IEEE Emerging Trends in Electrical and Computer Technology (ICETECT), Nagercoil, India, Vol.23,No.24 , 2011.

[14] Ren, S. Deligiannis, N. Andreopoulos, Y. Islam, and M. Schaar. "Dynamic Scheduling for Energy Minimization in Delay-Sensitive Stream Mining", IEEE Trans Signal Process.Vol.62,No.20, pp. 5439–5448, 2014.

[15] Retter, T. L.,and Rossion. "Uncovering the neural magnitude and spatio-temporal dynamics of natural image categorization in a fast visual stream", Neuropsychologia.Vol. 91, No.1, pp. 9–28, 2016.

[16] Luo, Y., Guan, Y. P. "Adaptive skin detection using face location and facial structure estimation", Iet Computer Vision. Vol.11,No.7,pp. 550–559,2017.

[17] M. Bilal. "Algorithmic optimisation of histogram intersection kernel support vector machine-based pedestrian detection using low complexity features", The Institution of

Engineering and Technology, Vol. 11, No.5,pp. 350 – 357, 2017.

978-1-7281-0757-8