International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(2): 166-176
The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-001

Cyber Security Platform Solution Based on the Facial Imaging and Fingerprinting

[1]SulaimanAlshebli, [2] Fatih Kurugollu, [3]Mahmoud Shafik:
University of Derby
Emails: [1]s.alshebli1@derby.ac.uk, [2]f.kurugollu@derby.ac.uk, [3]mshafik@derby.ac.uk

Abstract:
The recognition system based on iris images is costly and requires high resolution optical sensors and camera systems to aid security professionals at the time of authentication and verification. The fingerprint recognition system may not be as complicated as iris recognition system, but it requires individual physical contact at the time of identification. Iris recognition is more accurate than fingerprinting. The facial image can change depending on how the subject is sitting however, the shape and structure of the facial skeleton, location of the eyes, mouth, and nose remain unchanged. Due to this remarkable characteristic and ability to generate the facial image features with near perfect identifiers and the lack of requirement for physical contact with the recognition system makes the facial recognition system unique. The development of a complex facial recognition system using this approach could be used to identify unauthorized users and hackers and greatly improve cyber security processes. The features can be obtained from processing information stored on videos or facial images captured from the scene even without contact. Many recognition systems have been developed over the last fifty years, but one of the most accurate and fastest methods for identifying faces is based on the Eigen Analysis of facial features.
In this research program a hybrid technique for personal recognition based on facial imaging and fingerprinting, using Discrete Wavelet Transform (DWT), is proposed and applied on Facial imaging and Fingerprinting images to create a compressed coded version of the information. Then, Singular Value Decomposition (SVD) is applied on the coded image to find the Singular Values (SVs) of the coded image as the recognition feature. Once each SVs vector is formed, both vectors will be merged to obtain final feature vectors for recognition. The feature vectors will be used to compare against all other feature vectors stored in the database to find the best match or no match. Three-level cryptography (scrambling, transformation and XOR operations with a secret key) will be used to secure the features vectors prior to storage on the databases or the cloud computing facilities.
All feature vectors are stored inside our Facial Imaging database. During the identification process the algorithm will calculate all sub-image features and form a feature vector to be compared with existing feature vectors inside the database. The Euclidean Minimum Distance has been used to obtain the best match for the target image amongst the source images and print the closest images or no match message. The initial research results and findings clearly indicate that the new hybrid method for individual recognition based on the DWT and SVD has greater results compared with DCT, DWT or PCA methods.

Keywords: Biometric, Fingerprint, Facial recognition, Authentication, Feature Extraction, Singular Value, DCT, DWT, SVD, PCA, Cryptography, Compression.

Introduction:

The invention of high-speed digital computers and advancement in Information and Communication Technology (ICT) helped to move enormous amounts of information and data from daily life over cloud computing facilities, local and national networks. The information stored on cloud computing facilities, storage devices, databases and even during transmission must be secured using reliable and fast cryptography. In addition, networks, data centers, research facilities, military sites and all other network systems that contain vital information must be protected from intruders, illegal users and hackers. The traditional recognition systems used in cyber

security authentication were based on passwords and other information which are not related to the extracted features from individual biological characteristics and cannot be reliable because some of the secret keys and passwords could be forgotten, guessed, generated or even be stolen. The physical plastic card, smart cards, tokens and other additional items required for recognition may be lost, stolen or reproduced by thieves and illegal users. The features extracted from the individual biological characteristics cannot be stolen, misplaced, forgotten, or forged. The recognition system based on the individual features such as fingerprints and facial images are more reliable than traditional recognition systems because a human presence is required at the site and other information it is not necessary to be stored or memorized for accessing security systems [1-4].

The biometric authentication and recognition based on the features obtained from individuals are the most reliable technique of authentication and recognition because most of the individual characteristics and traits i.e. facial images and fingerprints are unlikely to change for a period of time. Cyber security has encountered many challenges especially when intruders have learned how to use the advanced technology and sensitive substances to build fake identification tools such as replicated fingerprints, imitation faces and even (fake) iris prints on cosmetic lenses to fool the systems and breach security.

Although the biometric recognition systems based on the iris images were the most reliable, the requirement of complex camera systems with high resolution sensors, robust and fast algorithms, along with the physical contact of the individual has made the iris recognition system very costly and troublesome. In contrast, the facial recognition systems may not require the presence of the individual at the recognition site because the facial image can be captured from a database of photographs or uncontrolled video or from surveillance cameras without physical contact, long before the individual reaches to the recognition system. Thus, the biometric recognition system based on facial images is still promising in spite of its challenges and limitations due to individual aging problem, facial expression, partial occlusion, light illumination and so on. The fingerprint information capture can be easily done by one scanner and it does not require complex sensor detection systems or complex camera systems required for iris recognition.

Humans have high perception in facial recognition even when the individual changes their appearance when relatives and friends can still easily identify that person. Building intelligent and smart systems with the capability and perception for facial recognition is still an ongoing problem and there are a number of research programs under development. The human perception is amazing and so far, no one has built a facial recognition system with the same rate that recognizes the individual face in every critical condition. Application of facial recognition includes video surveillance, automatic indexing of images, passport and visa verification, driving license verification, comparative exams, government and private sectors, voter fraud, FaceID and advanced human-computer interaction. Apple Inc. released the iPhone X with Face ID on November 3, 2017 with facial recognition capability to perform the biometric authentication that permits only the owner to access the mobile device [5-9].The Face ID relies only on the unique characteristic of the owner's face in which it scans the face accurately and compares with the stored facial image and recognizes the owner at all times even in different lighting conditions and with some changes in appearances. The biometric feature is important because individual characteristics do not change quickly over time and they do not need to memorize sequences of secret codes or other information necessary for identification and authentication. New biometric systems have the capability to identify individuals very quickly and they provide us with the accurate, reliable and low-cost solutions.

This paper contains 10 sections as follows:

1-Background on facial imaging –fingerprinting recognition.
2-Individual identification based on facial imaging – fingerprinting
3-Cyber security based on facial imaging –fingerprinting.
4-Advantage of biometric identification over others.
5-Proposed identification based on facial imaging – fingerprinting.
6-Proposed cryptography for securing features.
7-Methodology of the identification process.
8-Experimenatl results and discussion.
9-Conclustions.
10-Future work and proposed application.

1. Facial Imaging and Fingerprinting

Many researchers have worked on the area of individual recognition systems based on facial or fingerprint images. However, the pioneers of automatic facial recognition are Timbered Bledsoe, Greg Helen Chan and Charles Bisson. Helen Chan, and Charles Bisson also used computer algorithms to identify human faces and they obtained several good results for recognition (1965-1966) but they were unable to publish their research work due to some restrictions on the disclosure of intelligence [10-11]. They created a large database of images and their algorithm was designed to select the target image and compare it with those images which were stored in the database. Their algorithm was used to calculate the ratio of some responses regarding the distance of their eyes and the distances from their mouth as well as other characteristic measurements. The success of this method can be measured in terms of the ratio of response for all predefined characteristics when compared with the characteristics of all images stored in the database.

Although their method was successful they indicated that their method would not work properly and might create false recognition if there is image rotation, tilt, light intensity, angle, facial expression, aging and more. But, in particular, the relationship between two images of a person with two different head rotations is very small. The operator automatically extracts the coordinates from features such as the center of the pupils, the inner corner of the eye, the outer corner of the eye, and so on. Then a list of 20 distances such as mouth width and eye width were calculated for the recognition process. The process was time consuming and the operators can only handle approximately 40 images in one hour. Several systems have been developed by Christopher von der Malsburg and graduate students at Bochum University in Germany and the University of Southern California in the United States, as well as most systems developed by the Massachusetts Institute of Technology (MIT), and the University of Maryland. The Bochum System was developed by the US Army Research Laboratory and the software was sold and used by Zn-Face. The Zn-Face software was used by Deutsche Bank and international airports to identify the individual at the gates or other busy areas. The software had the capability to recognize individuals by facial images even though they have changed their facial features such as mustaches, beards, hairstyles, glasses and sunglasses.

Scientists and Engineers have faced challenges with the problem of individual recognition based on the facial image and fingerprint image. They have introduced new techniques to cope with new technology. In 2006 Vendor Face Detection Test (FRVT) and the Iris Challenge Assessment (ICE) were a major victory provided by the National Institute of Standards and Technology (NIST). Matching face recognition algorithms have proven that the advanced technology and new algorithm have increased the rate of recognition by twenty times since 2002 and tenfold since 1995. In fact, in the advanced face recognition algorithms many features have been extracted and methods such as Eigen feature extraction based on the co-variance matrix of the face image, neural networks, dynamic link architecture, hidden Markov model, geometrical feature matching and template matching are used. The approaches are analyzed in terms of the facial features extracted and the method of classification that has been used for comparison of the target image and the stored images in the databases [12-14].

Eigen face is one of the most accurate approaches to facial recognition. It is also known as Karhunen-Loève expansion, in which the Eigen analysis of co-variance matrix for each image is calculated to extract its Eigen values by a famous technique called Principal Component Analysis (PCA) [15-18]. The Eigen values of the co-variance matrix can be used to compress the facial images to a smaller size or reconstructs the facial images from more dominated Eigen values where the smaller Eigen values are ignored. Mathematically, the Eigen values and E Eigen vectors of the principal components of the facial distribution matrix or the co-variance matrix of the image can be calculated to decompose the image as linear combination of the all Eigen vectors. Any image can be reconstructed as the linear combination of all Eigen values and Eigen vectors because the set of Eigen vectors of the co-variance matrix are linearly independent However, it is possible to use only dominated Eigen values in image reconstruction where the smaller Eigen values are ignored. These dominated Eigen values can form a feature vector which can be used for image reconstruction or image recognition. The attractiveness of using neural networks can be due to its non-linearity in the

network in which the feature extraction process may be more efficient than the Karhunen-Loève linear methods. One of the first artificial neural network (ANN) techniques which was previously used for facial recognition is a layer-compatible network which contains a separate network for each stored individual [6]. The method of constructing the neural network structure is very important for successful recognition. It very much depends on the program you are looking for. For example, multi-layer perception and convolutional neural network have been applied for facial detection [19-23] and a multi-resolution pyramid structure is applied for facial verification [26-30].

Geometric feature matching techniques are based on computing a set of geometric features of a facial image. The author claimed that this technique can be accurate so that the facial detection is possible even with a resolution of at least 8x6 pixels when a single facial feature is hardly revealed in detail [31-33]. It implies that overall geometric configuration of facial features are sufficient for facial detection. The overall configuration is just a feature vector which consists of the position and size of the main facial features such as eyes and eyebrows, nose, mouth and facial features. The pioneer researchers in automatic facial recognition [34-36] have used the geometric features and achieved a peak performance of 75% recognition rate on a database of 20 people with 2 images per person, one as model and the other as a test image [37-40].

The first modern facial recognition system was developed in the late 1960's and early 1970's in which the geometric properties of the face were used for identification. Several features of the face such as both eyes, shape of mouth, cheek, and chin were selected to create a feature vector for identification. The geometric features of the face are good parameters for the recognition but they will perform differently at different light levels and they are considered as reliable features for recognition [13 - 41]. A reliable method of facial recognition can be obtained by using the Principle Component Analysis (PCA) of the facial image that reduces the dimension of the facial image vectors. The PCA method has shown good improvement compared with DCT, DWT and geometric features. However, the PCA suffers from the computational times due to its direct calculation of the Eigen values and Eigen vectors of the co-variance matrix of training images [41-48].

Fingerprinting has been used by humans as a reliable means of individual identification even long Before Christ (BC). Fingerprints have been found on ancient Babylonian clay tablets, seals, and pottery. Chinese records left from the Qin Dynasty (221-206 BC) have indicated that handprints have been used as evidence during burglary investigations. In 200 BC fingerprints were used to sign the written documents and contracts in Babylon. The chinese were the first nation to invent paper in 105 BC and they are also pioneers in using handprints and fingerprints on their documents. Iranian Physician Rashid Al-Din Hamadani (1247-1318) has mentioned in his book
(Jami. a Al Tawariجامع التواريخ) "Universal History", about the fingerprint as a means of signature and signing contracts during the Persian Empire. Dr. Nehemiah Grew was the first European who published a paper in "Philosophical Transactions of the Royal Society of London", 1684, and indicated about the ridge skin observations and fingerprints. In 1686, Marcello Malpighi, an anatomy professor at the University of Bologna, noted about fingerprint ridges, spirals and loops, where a layer of skin was named after him, "Malpighi layer". In 1823, Jan Evangelista Purkinje, anatomy professor at the University of Breslau, published his thesis discussing nine fingerprint patterns but he never mentioned that fingerprints can be used as means of individual identification. The British started to use fingerprints on 'native contracts', in July 1858, when Sir William James Herschel was the Chief Magistrate of the Hooghly District in Jungipoor, India. In July 1877, American microscopist Thomas Taylor proposed that finger and palm prints left on any object might be used to solve crimes. In 1882, Gilbert Thompson of the U.S. Geological Survey in New Mexico was the first person in the United States of America who used his own thumb print on a document to help prevent forgery. In 1888, Bertillon was appointed as the Chief of the newly created Department of Justice and he used the anthropometry as the primary means of identification and introduced the fingerprints as second category of special marks. In 1892, Inspector Eduardo Alvarez made the first criminal fingerprint identification, at Buenos Aires, Argentina, where a woman murdered her two sons and cut her throat to create a scenario to deceive the authorities. She tried to make it hard for investigators to detect her criminal action but her fingerprint on the door post proved her identity. In 1901, the Fingerprint Branch at New

Scotland Yard (Metropolitan Police) was created and one year later, 1902, Dr. Henry Pelouze de Forest suggested the use of fingerprints to screen New York City civil service applicants. Fingerprinting has evolved rapidly after the invention of digital electronics and computer facilities and presently fingerprint identification has been the most common means of identification and attendance registration in almost all offices around the world.

The most important challenge of cyber security is the presentation of fake samples at identification sites to act like a genuine client by fooling the recognition system in which the authentication process can be completed by fake fingerprints, printed cosmetic lens patterns, or even by face masks. The cyber security can be guaranteed by using the biometric authentication based on the facial-fingerprint features which would be obtained accurately by applying our proposed DWT-SVD method followed by three levels of cryptography to secure the feature vector prior to storing on a database.

2. Personal Identification Based on Facial Imaging and Fingerprinting

We have reviewed the previous works which have been done on feature extraction of both facial images and fingerprint images. The literature review revealed that the Principle Component Analysis (PCA) of the co-variance matrix can produce more accurate results in the individual identification as compared with DCT, DWT, artificial neural network, geometric feature extractions, and Hidden Markov Model. Researchers have shown that their enhanced SVD method has improved the accuracy of facial recognition as compared with Eigen faces, Fisher faces, and Laplacian faces. We have combined two methods of data compression, DWT, and feature extraction, SVD, to obtain our proposed hybrid model based on the feature vectors of both Facial images and Fingerprint images, called SVD-DWT faces. In this method we have extracted the features of both facial images and fingerprint images, in which the DWT algorithm is applied to reduce the size of the image matrix and create the DWT codes. Once the DWT codes are generated the SVD algorithm also applied on the DWT image codes to decompose the DWT matrix into three matrices, left singular vector, singular values, and right singular vectors. The Singular Values (SVs) will be used as extracted features which can be stored into the database for the future identification or can be used for comparison against existing features already stored. This algorithm can be implemented on mobile devices and tablets for personal recognition due to its high speed and accuracy that require less memory and CPU which is the limitation with most devices. The problem of most feature extraction algorithms is the time consumed for the detection and comparison but our method is fast and robust and can be replace the existing methods [25].

3. Cyber Security solution Based On Facial Imaging and Fingerprinting

The biometric system identification is very safe and could be considered the most effective method of individual identification because the biometric signatures are unique for each individual. The facial images and fingerprints are very accurate, easy to use, and the most economical biometric individual identification and personal computer user authentication technique. The data acquisition process is easy and only requires high resolution cameras for facial image capturing and a good quality scanner for fingerprint scanning. Fingerprint readers, iris scans and facial recognition have been used by high technology companies such as Apple Inc. which delivers significant advantages in the fight against cybercrime. Unfortunately, there are some risks in using biometric signatures such as the facial imaging, fingerprinting or even iris scanning because these systems can be hacked by cyber criminals trying to either steal or replicate the biometric data. In addition, clinics, health centers and hospitals which hold patient medical history, blood samples or DNA profiles must understand the security implications of a data breach and their potential liability. The biometric spoofing is the process of fooling a biometric security system using fake or copied biometric information. For example, a fingerprint can be stolen, copied and molded into artificial silicon to be used for unlocking a mobile device or accessing the user's bank account. The facial image can be copied on another smart phone and a photograph of the owner can be used for unlocking the device [24].

4. Advantages of Biometric Identification over Traditional Methods

The biometric system identification has many advantages over the traditional technique when the password or PIN numbers are used for accessing the network, making some transactions at ATM machines or passing through a secure door. If biometric identification is used it will reduce the likelihood of a

breach because the hacker algorithms cannot be used to retrieve keywords. It also eliminates the possibility of forgetting users' passwords. Biometric authentication can be applied based on the static models or dynamic in which the action is involved. The dynamics of writing one's signature as well as typewriting on the keyboard can be analyzed for the individual identification. Biometric signatures are vulnerable because the fingerprints of an individual can be captured from a glass of water and fool the scanning device at security gates or the image of a person can be copied by smart phone and use to fool the security system [32].

The following proposed techniques can be used to reduce the vulnerability of biometric signatures and increase the cyber security:

i- Encrypt the facial images or calculate their features before they are stored on the database.

ii- Encrypt the fingerprint images or calculate their features before they are stored on the database.

iii- Modify the identification system to be worked with Live Fingerprint images or Live Facial Images, in which the face and finger movements are required to capture the live images by using multiple high-resolution cameras.

5. Proposed Biometric Identification based on Facial Imaging and Fingerprinting

The research carried out in this article includes the design and implementation of a new identification system and basis for analyzing of the fingerprint & facial features. Once the features were obtained from face and fingerprint identification algorithms, we would store them in the databases for future identification. When an individual is approaching the security gate in which proposed algorithm is implemented, the facial image and fingerprint image of the individual will be taken by high resolution cameras and scanners. Then, our algorithm will compute the biometric feature vector of the individual and compare it with feature vectors stored in the database to find the exact match, best match, or no match for identification. We will design and implement an algorithm to get the characteristic of the Face and Fingerprint images by using DWT and SVD. First DWT is applied on each image to reduce the information and provide metadata rather than raw data. Then the SVD algorithm is applied to generate the singular values of the DWT coded data. The Singular values of face image and fingerprint image will be merged to obtain one feature vector for the comparison at the identification stage or storing on the database during the registration stage. We can apply our algorithm with 150 or more selected facial images along with the same number of related fingerprints to test the performance and the rate of the identification process as compared with other existing methods. Our hybrid method of the Facial-Fingerprint identification is new, unique, reliable and robust because its performance is based on the combination of the features obtained after applying DWT and SVD. Our proposed method can be used in retail stores or any other shopping centers to replace traditional credit card and PIN numbers with facial image processing for shopping and fingerprint processing for the final approval stage to complete the shopping process.

6. Proposed Cryptography for Securing Features

Our proposed algorithm is unique and based on two levels of data compression performed by DWT and SVD respectively, as well as three levels of security for applying encryption, based on the orthogonal transform matrices once the feature extraction processes are completed and prior to storing them on the databases. We have used the orthogonal transform matrices, such as DCT, Malakooti Transform (MT), DWT, Hadamard Transform (HT) to save the process time for matrix inversion during the decryption. The decryption process required inversion of the transform matrix and if the transform matrix is not orthogonal the inversion process would be time consuming and useless especially for real time processing. However, if we use the orthogonal transform for the encryption process the matrix inversion during the decryption process would be done easily and can be obtained by its transformation divided by a number which is already formulated. The time consumption for the process of orthogonal matrix inversion during the decryption stage would be negligible (order of one) as compared to non-orthogonal matrix inversion which requires direct calculation (order of 3).

The encryption of the extracted feature vectors is additional an security caution to protect the feature

vectors from unauthorized user or people who breach the security of the network and intend to discover the vital information stored inside the database or cloud computing storage facilities. The encryption has three levels of security and we can apply the first, second, or even third level of encryption security. First, we will scramble the information based on our proposed scramble algorithm. Then the scrambled data will be multiplied by an orthogonal matrix, such as Hadamard matrix or Discrete Cosine Transform and finally the transformed encrypted information will be XOR with the proposed randomized key gen values.
The result of our algorithm will be compared with the existing biometric authentication algorithms to compare the speed of operation, robustness and complexity of our proposed algorithm

7. Methodology:

To achieve the objective, the following research methods were used:

- Extracted the facial images and fingerprint images captured from high resolution cameras and scanners and saved them in to two separate files.
- Applied DWT on the extracted facial images and fingerprint images and saved them in to two separate files.
- Once the coded images are obtained from the DWT the facial images and fingerprint images are then applied to the SVD to obtain the singular values of coded facial images and coded fingerprint images.
- Merged the singular values of both combined DWT-SVD algorithms into a feature vector along with the individual ID for future identification.
- Encrypted the contents of the feature vector and saved them on the database for future retrievals.
- Developed an accurate and reliable biometric authentication system based on the facial-fingerprint images that is more operational, cost efficient and able to identify the individual with fake fingerprint or fake facial image at the recognition site.
- Identified the factors that need to be taken into account to implement cybersecurity solution based on the Face-Fingerprint images.

8. Experimental Results and Discussion:

Mohammad Sharif, et. al. [44] has shown that the enhanced SVD method has improved the accuracy of facial recognition as compared with Eigen faces, Fisher faces and Laplacian faces. We also applied our proposed algorithm on 150 face images from PIE facialDB along with 150 fingerprint images assigned to 150 individuals to test the performance and the rate of identification our hybrid method based on DWT-SVD. The results of the simulation shown in Table-1 are obtained from ratio of the number of recognized images over the total number of images in the database to calculate the accuracy.

$$\text{Accuracy} = \left(\frac{NR}{NT}\right) * 100\% \quad \text{(Eq- 1)}$$

Where, NR is the number of recognized images, NT is the total number of images in database.
The findings obtained in our method have been compared with other techniques and it has clearly shown the superiority of our algorithm over the existing ones as tabulated in Table-1.

Table-1: Comparison of the Proposed DWT-SVD Method with others using PIE Facial DB

Method	Accuracy	Percentage
Eigen Faces	121/150	86.66%
Fisher Faces	142/150	94.60%
Laplacian Faces	143/150	95.33%
Enhanced SVD Faces	144/150	96.0%
DWT, SVD Faces (Proposed Method)	148/150	98.66%

The results of the implementation have shown that the average recognition rate for Eigen Faces, Fisher Faces, Laplacian Faces were 86.66%, 94.60%, and 95.33% respectively. The enhanced SVD has improved the identification rate to 96.0% while our proposed method (DWT-SVD Faces) has a higher identification rate, 98.66% as compared with other techniques. We have also calculated the Mean Square Error (MSE) of facial image identification for four (4) images related to the same man but at different positions and light conditions as well as MSE of 4 assigned fingerprint image identifications.

$$MSE = \frac{1}{N}\sum_{i=1}^{n}(S_i - St)^2 \quad \text{(Eq- 2)}$$

Where, N is total number of images in the database, St is the singular value of the target image, Si is the singular value of the stored images.

The tabulated results, (Table-2 to Table-7), clearly show that our proposed method has a better performance in identification and results in the smaller MSE as compared with DCT as well as required less processing time, Table 5

.

Table 2-MSE of 4 Face Images from same Man

Session 3-Image-1	Image-1	Image-2	Image-3	Image-4
DWT	0	0.5781	3.7818	9.238
DCT	0	1.7891	8.4561	21.936
HT	0	0.0435	0.2871	0.3689
MT	0	0.0013	0.0023	0.0043

Table 3-MSE of 4 Face Images from same Man

Session 3-Image-2	Image-1	Image-2	Image-3	Image-4
DWT	0.4983	0	2.9841	7.9812
DCT	1.3256	0	7.3421	23.293
HT	0.0327	0	0.2171	0.3139
MT	0.0014	0	0.0018	0.0031

Table 4-MSE of 4 Face Images from same Man

Session 3-Image-3	Image-1	Image-2	Image-3	Image-4
DWT	3.4175	3.3242	0	5.4672
DCT	9.2356	7.4578	0	13.725
HT	0.1871	0.1464	0	0.2477
MT	0.0017	0.0016	0	0.0019

Table 5-MSE of 4 Face Images from same Man

Session 3-Image-4	Image-1	Image-2	Image-3	Image-4
DWT	8.453	8.237	5.874	0
DCT	17.145	17.981	12.787	0
HT	0.2318	0.3289	0.2278	0
MT	0.0046	0.0042	0.0028	0

Table 6-Process Time (in MS) of 4 Face Images

Session 3-Image 1-4	Image-1	Image-1	Image-1	Image-1
DWT	29416	29897	32914	35769
DCT	75915	77981	66891	75871
HT	57291	56891	54991	54895
MT	58734	58611	58321	52936

Figure-1: The Fingerprint Images of 4 Individual

Table 7-Process Time (in MS) of 4 Finger Prints Images

DB1-102 Fingerprints	Image 1	Image 2	Image 3	Image 4
DWT	29763	28943	31216	35734
DCT	74983	77823	66437	75341
HT	55351	55872	54983	54367
MT	58763	58991	58732	51818

9. Conclusions

We have determined a reliable, robust and fast technique for the calculation of individual facial recognition based on a combination of the DWT and SVD algorithm to obtain facial features for both registration and identification stages has been developed and presented in this paper. However, during the registration the symmetric cryptograph could be used to secure the captured facial features before being stored on the database. The encryption technique used three levels of security, scrambling by our proposed algorithms, transformation by using orthogonal transforms and XOR operation of the output of second stage with random number generator algorithm. This encryption process can be limited to one level or two levels instead of three if the speed of operation is important for real time analysis or a faster operation is required. However, the encryption process at any required level will increase the security of vital information before being stored on the local database or transmitted over networks to be saved on a cloud storage facility. The extracted features have been compared with the stored features on the databases to find the best match by calculating minimum distance technique based on the Frobenius Norm. The proposed algorithm minimises the cost and time consumption for calculating the facial-

fingerprint features as well as obtaining better resolution compared with the traditional algorithms, (Table-2 to Table-7).

Our algorithm can be used in retail stores for payment operations instead of using credit cards and PIN Numbers. We have suggested that for future work the research can expand our algorithm and use some criteria to select only the dominated singular values over the entire range of singular values to reduce the size of feature vectors which leads to saving storage space as well as increasing the process time for operations. We also believe that DWT can be replaced with either Hadamard Transform (HT) or Malakooti Transform (MT) for more accurate results for recognition but it might take more time operationally.

10. Proposed Application of Facial-Fingerprint Imaging

One possible future application for facial recognition systems is in retail stores. The cash register of the retail stores can be equipped with the cameras to obtain the facial images of customers during the transactions and ask them to use their fingerprints for final approval similar to what we are doing in the process of credit card and security PIN numbers. The recognition system should be able to switch from hybrid model of face-fingerprint identification to face and PIN numbers if the client's hand were to be broken or injured. This method of hybrid face-fingerprint is my proposed technique for the future of shopping at retail stores with high technology. Our proposed identification technique provides comfort for the customers to perform shopping without carrying any physical cards and without memorizing PIN numbers. This idea can be expanded to hotel reservations, eating at restaurants, buying train or airline tickets, renting a car, or paying hospital bills.

11. References:

[1] A. Alice Nithya, Dr. C. Lakshmi," Iris Recognition Techniques: A literature Survey", School of Computing: SRM University, July 30, 2016, https://www.researchgate.net/publication/282296433.

[2]ZdravkoLiposcak and Sven Loncaric," Face Recognition from Profiles Using Morphological Signature Transform", 1999.

[3] N. Popescu-Bodorin, V.E. Balas, "AI Challenges in Iris Recognition: Processing Tools for Bath Iris Image Database", Recent Advances in Automation & Information, SpiruHaret University/ AurelVlaicu' University, Romania, June 2010.

[4]Jin Ok Kim1, Sung Jin Seo2, and Chin Hyun Chung2, "Real-Time Face Recognition by the PCA kffB(Principal Component Analysis) with Color Images Book," 2004.

[5] H. Mehrabian, "Identification of the Identity based on the Iris Signal Analysis", Senior Project, Tehran university, Tehran, Iran, 2015.

[6]L. Sirovich and M. Kirby, "Low-Dimensional procedure for the characterization of human faces," J. Optical Soc. of Am., vol. 4, pp.519-524, 1987.

[7] T.K Sruthi , K.M Jini, "A Literature Review on Iris Segmentation Techniques for Iris Recognition Systems", IOSR-JCE, P- ISSN: 2278-8727Volume 11, Issue 1 (May. - Jun. 2013), PP 46-50.

[8]D. Yambay, J. S. Doyle, K. W. Bowyer, A. Czajka, and S. Schuckers," LivDet - Iris 2013 – Iris Liveness Detection Competition 2013", IEEE International Joint Conference on Biometrics, pages 1–8, September 2014.

[9] M. Kirby and L. Sirovich, "Application of the Karhunen-Loève procedure for the characterization of human faces," IEEE Trans.

[10] A. F. Sequeira, J. Murari, and J. S. Cardoso," Iris liveness detection methods in the mobile biometrics scenario", 2014 International Joint Conference on Neural Networks, (IJCNN), pages 3002–3008, July 2014.

[11] Krishna Prasad. K and Dr. P. S. Aithal, "Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image", International Journal of Management, Technology, and Social Sciences (IJMTS), ISSN: Applied, Vol. 2, No. 2, July 2017.

[12] V. Mura, L. Ghiani, G. L. Marcialis, F. Roli, D. A. Yambay,and S. A. Schuckers," LivDet 2015 fingerprint liveness detection competition 2015", In 2015 IEEE 7th InternationalConference on Biometrics Theory, Applications and Systems (BTAS), pages 1–6, Sept 2015

[13] D. Yambay, B. Walczak, S. Schuckers, and A. Czajka, " LivDet-Iris 2015 – Iris Liveness Detection", IEEE International Conference on Identity, Security and Behavior Analysis, (ISBA), pages 1–6, February 2017.

[14] Kirby and L. Sirovich, "Application of the Karhunen-Loève procedure for the characterization of human faces," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 12, pp. 831-835, Dec. 1990.

[15] L. Ma, T. Tan, Y. Wang, and D. Zhang, "Personal identification based on iris texture analysis", IEEE Trans. Pattern Analysis Machine Intelligence, vol. 25, pp. 1519,533, 2003.

[16] A. F. Sequeira, J. Murari, and J. S. Cardoso, " Iris Liveness Detection Methods in Mobile Applications", https://www.researchgate.net/publication/271516730, May 2014.

[17] M. Turk and A. Pentland, "Eigen faces for recognition," J. Cognitive Neuroscience, vol. 3, pp. 71-86, 1991.

[18] A F. Sequeira, H.P. Oliveira1, J. C. Monteiro, J.P. Monteiro, and J. S. Cardoso, "MobILive 2014 - Mobile Iris Liveness Detection Competition ", 2014, https://www.researchgate.net/ publication/271516334

[19]S.H. Hsieh , Y.H. Li 2, W. Wang , and C.H. Tien **, "**A Novel Anti-Spoofing Solution for Iris Recognition Toward Cosmetic Contact Lens Attack Using Spectral ICA Analysis", Sensors **2018**, 18, 795; doi:10.3390/s18030795, March 2018.

[20] .J. Stonham, "Practical face recognition and verification with WISARD," Aspects of Face Processing, pp. 426-441, 1984.

[21] G. Tamilmani , M. Kavitha , K. Rajathi, " Efficient Iris Recognition using GLCM and SVM Classifier", Journal of Industrial Pollution Control 33(2)(2017) pp 1566-1570.

[22] F. Pala, B. Bhanu, "Iris Liveness Detection by Relative Distance Comparisons ", CVPR, 2017.

[23]]J. Weng, J.S. Huang, and N. Ahuja, "Learning recognition and segmentation of 3D objects from 2D images," Proc. IEEE Int'l Conf. Computer Vision, pp. 121-128, 1993.

[24] D. Tang, Z. Zhou, Y. Zhang,K. Zhang, "Face Flashing: a Secure Liveness Detection Protocol based on Light Reflections", Network and Distributed Systems Security (NDSS) Symposium 2018, 18-21 February 2018, San Diego, CA, USA.

[25] S.D.R Kumar, K. B. Raja, R. K. Chhootaray , S. Pattnaik, " ",PCA based Iris Recognition using DWT", Int. J. Comp. Tech. Appl., Vol 2 (4), 884-893.

[26] S. Tamura, H. Kawa, and H. Mitsumoto, "Male/Female identification from 8_6 very low resolution face images by neural network," Pattern Recognition, vol. 29, pp. 331-335, 1996.

[27] H.K. Rana, M.S. Azam, M.R. Akhtar, "Iris Recognition System Using PCA Based on DWT", August 2017, SM J. Biometrics Biostat. 2017; 2(3): 1015. [28] L. He,H. Li, F. Liu, N. Liu, Z. Sun, Z. He "Multi-patch Convolution Neural Network for Iris Liveness Detection", National Natural Science Foundation of China (Grant No.61403389), (WACV), (Lake Tahoe, USA), March 2018.

[29] T. Kanade, "Picture processing by computer complex and recognition of human faces," technical report, Dept. Information Science, Kyoto Univ., 1973.

[30]J.Yotipoonia, P.Bhurani, S. K. Gupta, S.L. Agrwaj, "New Improved Feature Extraction Approach of Iris Recognition", International Journal of Computer Systems.2016; 3: 1-3. 16.

[31] .J. Goldstein, L.D. Harmon, and A.B. Lesk, "Identification of human faces," Proc. IEEE, vol. 59, pp. 748, 1971.

[32]S. Boukhonine, V. Krotov, and B.Rupert "Future Security Approaches and Biometrics", CAIS, Vol. 16, 2005, Page 937- 966.

[33]Y. Kaya and K. Kobayashi, "A basic study on human face recognition," Frontiers of Pattern Recognition, S. Watanabe, ed., pp. 265, 1972. [34] D. Menotti, G. C. Chia, et al, "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection", IEEE Transactions on Information Forensics and Security, Volume: 10, Issue: 4 , April 2015,http://dx.doi.org/10.1109/TIFS.2015.2398817.

[35] A. Czajka, K.W. Bowyer, "Presentation Attack Detection for Iris Recognition: An Assessment of the State of the Art ", ACM Computing Surveys on June 13, 2018.

[36] Javier Galbally, A.G.Barrero," A Revie of Iris Anti-Spoofing ", 978-1-4799-8105-2/15, 2016 IEEE.

[37]D.Yambay, B. Becker, et al. "LivDet Iris 2017 - Iris Liveness Detection Competition 2017", Clarkson University, USA; University of Notre Dame, USA,…, and Inst. of Automation, Chinese Academy of Sciences, China, 2017.

[38**]** E. Wolff, Anatomy of the eye and orbit, 7th edition. H. K. Lewis & Co. LTD, 1976.

[39]S. Alshebli, M. Shafik, F. Kurugollu, "The Cyber Security Biometric Authentication based on Liveness Face-Iris Images and Deep Learning Classifier", ICIA 2019, July 2019.

[40] Aertec Solutions, "Biometric Identification at Airports", 27/03/2017, https://www.aertecsolutions.com/2017/03/27/biometric-identification-at-airports/?lang=en.

[41] S. Kumar Singla, P. Sethi," Challenges at different stages of an iris based biometric system", Songklanakarin J. Sci. Technology, 34 (2), 189-194, Mar. - Apr. 2012.

[42] K.K. Sung and T. Poggio, "Learning human face detection in cluttered scenes," Computer Analysis of Image and patterns, pp. 432-439, 1995.

[43] .Engelking, " Fingerprints Change Over the Course of a Person's Life", DARPA, June 29,2015.

[44] Komal, Dr. C. Kant," Liveness Detection in Different Biometric Traits: An Overview "International J. of Adv. Research in Comp. Sc., Volume 8, No. 5, May – June 2017.

[45] John Trader, "Biometrics: How does it Reduce the Risk of Security Breaches".

[46] S. Lawrence, C.L. Giles, A.C. Tsoi, and A.D. Back, "Face recognition: A convolutional neural-network approach," IEEE Trans. Neural Networks, vol. 8, pp. 98-113, 1997.

[47]Nic Fleming, "Fingerprints can reveal race and sex". The Telegraph, AKA The Daily Telegraph, London. Telegraph Media Group Limited, October 27, 2018.

[48]DavideMaltoni, Dario Maio, Anil K. Jain &SalilPrabhakar, Handbook of Fingerprint Recognition. Springer Science & Business Media, 2009, ISBN 9781848822542.