The Cyber Security Biometric Authentication based on Liveness Face-Iris Images and Deep Learning Classifier

SulaimanAlshebli, Mahmoud Shafik, Fatih Kurugollu
University of Derby, UK
sulaimanalshebli@gmail.com, mshafik@derby.ac.uk

Abstract:
This paper explains the liveness detection of the biometric system using the Face-Iris Images and deep learning classification. We have proposed novel hybrid algorithms for Face-Iris Liveness Recognition which can be used in cyber security authentication.In proposed model the individual identification is obtained from the extracted features that captured from face-Iris Images. Iris recognition is one of the most important biometric traits in which the iris image will be processed by some type of reliable, robust, and fast algorithm to capture the unique features embedded in iris. The camera system in which is used to capture the iris image will register depicts changes and variations in size of Iris as exposed to the light during the checkup and individual identification. This information will be used to verify the liveness of the iris image and distinguish the real lived iris image from the faked iris image.
The recognition system based on the iris images are costly and required high resolution optical sensors and camera system beside the presence of the individual at the time of authentication and verification. The face image may change in certain degree such as appearance but shape and structure of face skeleton , location of eyes, mouth, and nose are remain unchanged. Due to this remarkable characteristic and ability to generate the face image features with near perfect identifiers and lack of requirement for physical contact with recognition system has made the facial recognition system remarkable.
Our proposed face-iris feature extraction has been used to detect the fake face or iris from the real one and genuine live iris from the printed iris information by using the cosmetic lens. Our proposed model is based on the iris and face images in which high resolution camera and sensors are required at site to distinguish liveness Iris from fake one along with the high resolution algorithms that use combinations of DWT and SVD. The findings and results have shown the superiority our method,DWT-SVD, compared with hybrid of DCT, HT, MT with SVD, respectively. Our algorithm could be used to identify the fake Iris and face and greatly improve the cyber security. The extracted features can be obtained from videos or face images which have been captured from the scene even without individual physical contract.
Our proposed model has been used for authentication and identification of the individuals based on the extracted features obtained from a new hybrid algorithm using both SVD and DWT.In proposed algorithm the face-iris features have been extracted and they are saved in the face-iris feature vectors for recognition. The Euclidian Distance vector has been used to classify the feature vectors extracted from live and fake face-iris images.
The result and comparison of the proposed face-Iris recognition based on DWT-SVD with other technique has shown. Our method not only has higher speed of operation compared with other techniques but its rate of recognition is also good s as shown in the tabulated results.Experimental results also have shown that the hybrid methods of MT-SVD and HT-SVD have a better recognition results compared with DWT-SVD but their complex computation and extra time requirements for real time systems make them less important that DWT-SVD.

Keywords: Biometric, Presentation Attack, liveness Detection, Face recognition, Authentication, Contact Lens, printed patterns.

1. Introduction:

1.1Biometric Identification and Characteristics:

The identification of the people has been the human interest from ancient times, but with the advancement of technology the activities and encounters of the individual also have developed which required the modern identification systems for the human

recognition. The passport control, automatic banking system, personal identification based on the driver license, student identification card, grocery shopping using checks or credit cards and so many other cases exist that individuals must be identified before some services are given or some transactions are permitted to be performed. In old day, the passport information, passport picture, and stamps of the issuing government were the only means that could be used for individual identification in international airports. The passport details and including the passport booklet could be easily purged and falsified because none of this information was depend on the individual characteristics.

When the identification is involved with individual characteristics which captured from human body, such as finger prints, iris image, face image, voice, and so on, then the method could have better performance and would be both unique and easy to measure even with the changes over the time. Biometric identification techniques which identify individuals based on the physiological or behavioral characteristics are unique which depends on the human body to diagnose or confirm the individual and is more reliable than conventional methods because they act on the basis of what you are and not some details that is known to the individual, such as ATM Personal Identification number (PIN)[1]. Since, the debit card can be stolen and the PIN number can be captured through the hacking or can be handled by someone else, then the conventional method is highly vulnerable to misuse by hackers, thieves, and intruders. Biometric systems are usually used for purposes of control the entry and exit of individuals during the banking transaction. The rate of fraud and misuse in biometric identification is less than to the conventional identification and it can be considered as the ideal case for the individual identification.

1.2 History of Facial Recognition System:

Face recognition system is the one of most famous method of biometric recognition and several researcher, scholars, and scientist have work in the area of facial recognition but most of credit should be given to Woody Bledsoe, Helen Chan Wolf, and Charles Bissonwho were the pioneers of the automated facial recognition. They have used computer algorithms to identify the face recognition but could not publish their work due to public restriction for revealing intelligent information. They have created a massive database of images and photograph and their algorithm used to find features of the target image and compare it with features of existing images inside the data base to find the best match among them. The criterion of success was based on the ratio of the answer list over the total number of images on the database. Their algorithm could hardly identify the target image among recorded images where target image had problems of light intensity, aging, facial expression, rotation, and so on.Their face recognition algorithm extracted feature such as the distance between the center of pupil, width of mouths, dimeter of eyes, and so on. Their work continues by Peter Bind, at Stanford Research Institute and several facial recognition systems were developed by Christopher von der Malsburg and his students at University of Bochum in Germany, and researches in University of Southern California, Maryland and MIT in USA [7].

In the early 1970's, the first semi-automated facial recognition system was developed based on the geometrical information where a few landmarks were placed on the image to locate the major facial features such eyes, nose, mouth, chin, cheeks, and so on. When the locations of the facial features are marked then a few distances and angles were calculated form these landmarks to create a feature vector for the comparison process. Yuille et al. [18] measured the facial features using templates of single facial features and mapped them onto a global template. During the first stage of facial development most of the techniques were based on the automatic detection of the individual facial features. The face recognition based on the geometrical feature-based methods is insensitive to light illumination but the extracted features are not reliable enough for face recognition [11, 14]. This method later was abandoned and replaced by holistic color-based techniques in which it aligns a set of different faces to obtain a correspondence between pixels intensities and a nearest neighbor classifier can be used to classify new faces [12].M. Turk and A. P. Pent Land have developed face recognition based on the Eigen values of the face image which was called the Eigen face [15]. In Eigen face technique the pixel intensities of the target image will not compared with the pixel intensities of the stored images but instead the Principal Component Analysis (PCA) will be used to extract the features of the target image and reduce the

size of the comparison vectors. One of the Eigen face methods that widely has used is the technique of Fisher face [8, 10]. In this technique the Eigen face is combined with Fisher Linear Discriminant Analysis (FLDA) to obtain a better performance for identification of the face image. In Fisher faces, the PCA has been used to reduce the dimension of the target image intensity and then the FLDA is applied to obtain the optima projection for the separation of the faces from different persons. Several techniques have been proposed after the introduction of Fisher faces in which the new techniques even have provided a better projection for the separation of the target image from different persons. The most famous algorithm similar to the Fisher face is Kernel Fisher faces [16], discriminative common vectors [9], or Laplacian [13]. Other methods of face recognition are based on the neural networks [19], Gabor wavelets [20] and active appearance models [21-23].

Over fifty years, the face recognition system has developed constantly and it has massive improvement on both hardware and software. With existence of the smart phone and surveillance camera the facial recognition system also has developed at the same rate of intelligent video solutions. Facial recognition is used widely today for identification of individual at international airport for passport verification, enforcement and border patrol, counter terrorism, department of motor vehicles, locating the criminal and dangerous people hidden in cities, exam fraud detection, reduce ATM fraud, and even use face as loyalty card.

1.3 Methods of Face Recognition:

The face recognition technique can be classified into two separate techniques dynamic (no video) and static (video). The process of dynamic recognition is employed when we have a video sequence in which the background image is much cluttered and there is more than the target image in face image scene. Since the video sequence is available we can apply the motion to segment faces of moving persons. In static image recognition we will use the image with controlled illumination, resolution, background, even distance between camera, 3-D Scanners, and the person. Some of the image which emerges in this technique can be obtained from a video camera. In this research we have used the static face recognition based of the Extracted Feature Vectors obtained from SVD of face sub images and compared our results with Face Recognition methods based on the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), and Principle Component Analysis (PCA). Finally we combine the SVD and DWT methods to get higher resolution for highly secure sites in which the risk of breath to cyber system is very high. In this hybrid method three-level DWT will be executed on the face image and the then SVD is applied on the third level of DWT coefficients.

1.4Iris Promising Role in Biometric Identification:

The iris recognition is considered to be one of the most reliable and promising biometric method due to its characteristic. Iris plays a major role in human vision and object recognition as well as a good source of individual identification because its physical characteristic remains unchanged from fetal life to life [25]. The iris tissues are virtually hard to reconstruct from any substances and make it almost impossible for hackers and intruders to build fake iris tissues. In Iris identification the physical characteristic of a person are taken by the device and its coded features are extracted and compared with the stored codes in the database and identification can be done when the rate of identification is in the range of predefined threshold value. The conventional recognition will not provide any false identification because the identification is based on the physical card and password number and the exact value leads to the identification. But, in iris recognition no physical card is required and no password need to be memorized or retained but the presence of the person is required to capture the individual iris features for authentication. This system may provide false identification by rejecting the real individual when there is noisy environment during the capturing Iris Image. Biometric recognition systems, especially iris identification have two important features that make them more reliable and feasible. First, the person who wants to be identified by security systems must be personally available at the time of authentication. Second, the identification process does not require that the person retains the information or memorize the secret password for the authentication process, because the identification is based on the individual characteristic [2].The iris identification system involves a pre-registration phase in which the Iris

images are captured by the system and the coded features are extracted after some process and the results are saved inside the database. Once the coded features are stored inside the database then the person can be verified by the system.

1.5 The Characteristics of the Iris Recognition:

Iris recognition is an automated method of biometric identification in which the identification process carried on by applying the mathematical pattern recognition techniques on the video image of one or both of the Irises of an individual's eyes. Iris image is a reliable identifier which can be used for individual identification and has the following characteristics: Uniqueness, Extraction, High Resolution, and Stability [3].

1-**Uniqueness**: The feature of each person individually will be distinguished from feature of other person and the features are unique.

2-**Extraction**: The features are customized and they can be easily obtained with high speed algorithms without the need of lots of processing.

3-**High Resolution**: The difference between features of two individual is so much that they can be easily distinguished without a lot of effort.

4-Stability: The extracted features will not change due to the times and age of individual from fetal life to the end of life.

The scientist and health professional has suggested the amazing unique characteristic of Iris image as early as 1950s but it was not used for a long time due to lack advanced technology for camera system, capturing sensors and recognition algorithm. Recent algorithm used for the Iris ID scanning can capture 240 unique features in an iris image which is about 5 times as many as fingerprint images. The error rate of the Iris recognition is far less than other than biometric techniques such as fingerprint or face recognition systems.

1.6What are the Challenges in Iris based Recognition:

The iris recognition system has been used for individual identification and authentication and iris images are captured from human eyes without any physical contact or intervention. This recognition system is widely used at international airport gates and main entrances of highly protected data centers and military zones where the high level of security is required for accessing the system or passing through the gates. Iris images are highly reliable due to its characteristic of uniqueness, stability, extraction, and high resolution characteristics but still many challenges exist in the recognition system. The most important challenges in iris based recognition are in sensor module, preprocessing module, feature extraction module, feature matching module, and liveness [27]. In sensor module the identity recognition will be reduced significantly when the iris images are not scanned perfectly due to problem of lighting, motion blur, or occlusion. Those recognition systems which have employed the fixed-focused optical lens may generate the defocused iris images. Iris scanners work properly when the targets are stationary and any target movement during the scanning may cause the iris images to be blurred.

In preprocessing module the iris localization and iris image quality evaluation are the most important steps of recognition which involved in the detection of the inner and outer boundaries of the iris image. The first action of localization algorithm to detect the pupil, usually black circular part, from surrounding iris tissues and get iris image. The next step is to convert the iris image to the binary image using some the histogram analysis of the iris image. The localization algorithm and binary image conversion must be done accurately to prevent the iris image degradation. The feature extraction and feature matching are two crucial steps of the iris recognition that need to be done accurately and precisely. The feature extraction and feature matching are the most concerned stages of iris recognition system which their speed and accuracy depends upon the type of feature extraction algorithm and the distance metrics. The most important problem of the feature-based iris recognition is the result of matching performance which has significantly influenced by many parameters during the feature extraction process such as camera resolution, effect of visible light to individual eyes, and so on. The contact lenses with a printed patterns or printouts of the iris are other challenges of iris recognition system which can be used to deceive iris identification and bypass the security system. To prevent such spoofing attack it requires the additional high resolution sensors and accurate algorithm for the iris liveness detection. This paper consists of 9 sections: Introduction, Literature Review, Iris Liveness Recognition Techniques,

Cosmetic Contact Lens and Iris Noise Reduction, Data Set Contributions and Algorithms, Methodology, Experimental Results and Discussion,Conclusions and Future Works, References.

2. Literature Review:

Biometric recognition based on the Iris Identification is a reliable, unique, and robust identification method in which the data are captured from iris image of individuals and then processed by reliable and fast algorithms for the feature extraction. Once the process of the feature extraction is completed then the extracted features are compared with the iris features stored in the databases, and the individuals are identified when the results of the comparisons are within the accepted range of the Threshold. Since, the human iris is unique similar to the fingerprint it can play a major role in the cyber security system and cloud computing for accessing the protected networks or physically reaching to the heart of data centers where the vital information are stored, or even protecting the database from the intruders and hackers. Most of the security verifications and checkup systems in International Airports have been focused on the iris information which is collected automatically from individuals while they are within the range of Iris camera [26]. This method, although in a non-volatile optical environment, the distance between the eyes and the motion of the subject is still not very precise, but is now used in a number of countries around the world.

The iris development has begun from the third month of embryonic life. The unique pattern of iris has started to develop in the first year of life but the pigmentation of the stromal layer is stabilized in the first few years of life. The formation of iris tissue is random and not related to genetic factors and the only agent in the iris that depends on the genetic factors is the pigment cells. Two eyes of one person have completely independent tissues in the iris and also eye tissues of twins are different. Identification based on iris images involves analyzing the characteristics of the colored tissues of the eye which are enclosed between the pupil and the iris. Complex iris tissues can includes specific features and abundance such as grooves and bulges, zigzag texture, loops and spots. An iris scan can be obtained from an average and normal camera which does not require the individuals have close contact with the camera and the camera. This contact independent Iris system makes it unique in comparison with other biometric identification systems. The Iris image from one person to another is totally different because there are many different tissues that are located around the pupil. These unique patterns make the Iris image to be more unique than fingerprint image and be the most important reliable element of the biometric system. The iris scan for a person who is wearing glasses in the eye or using the contact lens can be easily done and device can correctly identify the individual identity [5].

The Iris is an internal and protected tissue that is isolated from outside but it can be seen clearly from outside. This property makes the Iris to be an appropriate tissue for diagnosis and its identification mechanism has been considered by the researchers and scholars.But, the Iris pigments may have changed and become more complete before the early years of life [6].

There are several different image processing methods for extraction of features from unique properties of Individual Iris by converting the Iris image into a biometric code. The biometric code is the result of applying mathematical operators to the iris image. The codes obtained from the individual Iris images will be stored in the database when they are extracted from the Iris code generation algorithm. When Iris system is used to identify the individual the Iris image of individual will be taken from the camera system and the code generation algorithm installed in the system will create the Iris code. This Iris code will be compared to the Iris codes of the stored in database and the distance measures are calculated. The system will look at the code that generated the least distance measured with the code obtained from the person. If the distance measure code of individual Iris image is equal or less than the threshold value, the person is diagnosed by the Iris system otherwise the person is not recognized[7].

3. Iris Liveness Recognition Techniques:

Biometric recognition is the best alternative technique for the password based authentication system in which the live characteristic of the individual will be used instead of the password. In conventional system the password and some other information is required to access a secure network system or pass through some security gate at research centers , international

airports, military zones, or nuclear facilities. Despite the popularity of the biometric systems, their reliability, and requirement of the physical presence of the individual at the security check point, these system are also vulnerable to spoof attacks, presentation attacks, and all type of false presentation which have been used by intruders to deceive the systems and bypass the security check process. One way to protect the biometric systems from any attack is integration of the liveness detection system and installation of additional high resolution sensors to the biometric system to be able to distinguish between the fake sample presentation and real one at the sensor level. The liveness detection hardware and software facilities have the capability to recognize whether the presentation sample at sensor level is alive or fake.

Face image, fingerprints, and iris images are the most useful biometric characteristics elements that have been used in biometric recognition systems and they are vulnerable to spoof attack but the iris images are more reliable due to the facts that liveness detection system can distinguish the lived iris or fake one easier than other biometric elements[28]. The liveness detection techniques regarding to the iris image can be listed as following: Pupil response, Motions of Eye Retina, reflection from Eyes, Detecting Edge Sharpness. The change in light illumination will change the size of the pupils and the living iris can be detected by measuring the change of pupil's size when the light illumination is changed. If the fake iris sample is presented then there would be no change in pupils size where the size of real iris sample will be changed about 5%-15% depend s upon the light intensity. When the real individual is in front of the camera system while the sample iris images are captured the motions of eyes retina can be detected while the fake eyes has no motion for eye retina. In addition there would be some reflection from human eyes while there is no reflection from fake eyes or dead human's eyes. The measurement of iris edge sharpness can help us to detect the sign of living iris while the fake iris edge is much sharper than living iris edge.

The fingerprint recognition is one of oldest identification technique that has been used to identify the individuals prior to the invention of computer and electronic devices. The fingerprint pattern for every individual is unique and even two identical twins have two different fingerprint patterns. The liveness detection technique used in fingerprint recognition to distinguish between the living fingerprints or fake one is based on pulse detection and anti-fraud biometric sensors. But the pulse rate of the individual is not fixed and it can be change due to stress, fatigue, emotion, sadness, happiness, and so on. So it cannot be used as reliable liveness detection because the intruder can have the pulse rate near the working range but the antifraud biometric sensor can accurately detect the blood flow rate through the fingertip.

4. Cosmetic Contact Lens and Iris Noise Reduction

The biggest challenge for Iris identification is noisy environment that produce low quality Iris image which is not appropriate for identification as well as the contact lens with a printed patterns or printouts of the iris that can be used to bypass the biometric security system. The first problem can be solved by using high resolution sensors that can be utilized to capture the good quality Iris image even in the noisy environment. This good quality Iris image may still has some type of high frequency noise and the process of high-pass filtering can be used to reduce the effect of noise. The second problem can be solved by the applying the hardware-based system or software- based system to detect the presentation attacks related to the contact lens with a printed pattern or printouts of an individual Iris image. In hardware-based system additional sensors will be installed to capture a good quality iris image and detect the presentation attacks. In software-based system additional signal processing algorithms will be apply on the captured Iris image to obtain the more reliable measurement to detect the presentation attacks. Both techniques will classify the input images as either a live real iris image or a fake image. The first and second International Fingerprint Liveness Detection Competition, Live Det 2009 and Live Det 2011 respectively, provided the assessments regarding to the software-based system for only fingerprint image, but the third International Fingerprint Liveness Detection Competition, Live Det 2013, expand the idea for both fingerprint and Iris image too. The Live Det 2015 was focused on both fingerprint and Iris image but the Live Det 2017 was solely concentrated on the Iris image presentation attacks assessment [8].

The people who have used the Cosmetic Contact Lens (CCL) with circular pigments, intentionally or

unintentionally, they will obscure the natural iris texture which caused the Iris image to become degraded and lower the result of resolution performance. Many algorithms have been used to develop anti-spoofing technique for Iris recognition, such as Adaptive Kalman Filter, Relax algorithm in Smart Grid. The anti-spoofing techniques can be divided into two different categories, (1) using a completely fake or printed Iris image to fool the security system and (2) modifying the texture of living Iris using augmented materials or wearing cosmetic contact lens. The Iris recognition system also is divide into two categories, (1) verify to see whether the eyes under test are alive (liveness detection), and (2) verify to see whether the eyes under test are wearing CCL. If the biometric recognition system verified that eyes under test are faked and not alive then the recognition will be terminated and system will reject the recognition process. But, if the system recognized that eyes under test are alive but with CCL, then the individual will be asked for cooperation to take the CCL off and recognition process will be repeated. S.H Hsieh, et al, [13] claimed that no one has developed any algorithm to perform Iris Recognition with success when the individual has used CCL. They have developed a hardware-software hybrid iris recognition system which deals with CCL-based spoofing. They have assumed that the Iris texture and CCL pattern are statistically independent in the spectral domain. Their proposed technique will combine a Dual-Band Camera (DBC) system with a source separation tools with the capability of separating the spectral components of the natural Iris region from the CCL's texture, by removing the CCL texture image from the mixed image. In this technique it is not required to remove the cosmetic contact lens during the recognition and the technique is called the recognition-based rather than detection- based system. F. Pala and B. Bhanu[14] have worked on the mobile Iris liveness detection system to solve the problem of spoofing attack, in which the printed image from an authorized user is presented to mobile sensor by a non-authorized user in order to obtain the illegal access. They have used the MobBIOfake dataset which is composed of 800 original Iris images and its corresponding fake Iris images, obtained from the printed images of the original one captured with the same condition. They have used deep learning methods based on Triple Convolutional Neural Networks (TCNN) that takes as input two real iris Images and a fake Iris Image or two fake Iris Images and a genuine Iris image. Their goal was to increase the number of training samples and generate a big architecture to be able to separate the original image from the fake one. The matching technique was obtained by computing the distance with respect to a reference set of real and fake images. Their proposed approach allows for real-time processing using a smaller network and provides equal or better than state-of-the-art performance on three bench mark datasets of photo-based and contact lens presentation attacks [15].

5. Data Set Contributions and Algorithms:

The paper by L. Ma, et al has made a number of contributions to the Iris identification techniques and became as the benchmark of standards for the Iris Recognition and establishment of the Iris dataset. The first Iris dataset, Chinese Academy of Science Institute for Automation (CASIA) is available to the Iris recognition community and has been widely distributed. In CASIA version 1, the preprocessing is applied to replace the pupils with a circular region of uniform intensity. The CASIA algorithm was developed to handle three types of Iris image: 1-A printed Iris image 2-An Iris Image with printed contact lens 3-A genius Iris image. The Iris image first has been passed through the SoopNet- 1 to detect whether the Iris image is printed or not. If the image is classified as live Iris sample, then it will pass through SoopNet- 2 to verify whether it is Live Iris or contact lens Iris. Another Iris liveness recognition algorithm, UNINA, is developed by the University Federico II of Naples to tackle the LivDet Iris Competition. The UNINA approach is based on the iris segmentation, dense feature extraction, and SVM classification. The Iris segmentation is performed by Canny edge detector and on the Circular Hough Transform. The dense feature extraction is more preferable in the security issues where we are interested to extract the features following a grid pattern as opposed to regular feature extractor that can extract the most information. The dense feature extraction does not look for information and just describes each point following a given pattern. The Iris recognition technique depends only on the extracted features from Iris image. Since the camera has taken the Iris image and image related to the

pupils then the pupils information should excluded from the Iris image by replacing the pupils with a circular region of uniform intensity. The differentiation will be done further by a classifier called Support Vector machine (SVM) which will filter out the Iris Image from the pupils' image [9].

The biometric systems have advantages over the classical security systems because in biometric systems the human characteristics are used for individual identity rather than somethings that individual knows or possess. But, biometric system also has their own problem of lack of secrecy, in which face, iris, or fingerprint of the individual can be stolen. In addition, biometric systems are vulnerable to external attacks, such as printout of Iris image, and contact lens with printed patterns which could decrease their level of security. The attacks can be classified as two main groups, direct and indirect attacks. The direct attacks refer to the possibility of generating the artificial biometric samples, such as fake fingerprint, face image, or iris image, in order to access the security system illegally [10]. These types of attacks are performed at sensor level and no other information is required about the system operation, feature extraction techniques, matching algorithms, feature vector format, etc. In indirect attacks the knowledge of system operation is required and usually this type of attacked will carried out by some virus like Horse Trojan that can be used to bypass the feature extractor and matching algorithms, or the database is manipulated and some information is added or deleted. To overcome these problems and reduce the vulnerability of the biometric security system the development of iris liveness detection techniques is crucial, especially with the revolution in the use of mobile devices in our daily life which has urged the liveness solutions in the mobile biometric field [11-12].

S.D.R Kumar, et al.[16], have proposed the Principle Component Analysis(PCA) based Iris recognition with Discreet Wavelet Transform(DWT). They have removed the upper and lower parts of the Iris image to reduce the effect of eyelashes and eyelids and then applied the DWT. They have created a covariance matrix from the coefficients of the DWT and then applied PCA. Once the features extraction completed, they have used multiple classifiers such as KNN, RF, and SVM for matching. Theirresult has shown that PCA-DWT Iris recognition method have abetter performance than the conventional algorithms.

H.K. Rana,et al. [17] have used the similar approach as S.D.R. Kumar, but they have applied the Hough transform for localizing the iris and pupil regions during the segment process as opposed to the histogram equalization on the Iris template. The summary of their method is given in last fivesections.

6. Methodology:

The Iris recognition systems consist of five steps: 1-Iris Image Acquisition 2-Iris image Segmentation 3-Normalization 4-Fature Extraction 5-Matching.

Once the Iris image is obtained, the segmentation is performed by using the Hough Transform (HT) for localizing the iris and pupil regions. The result of segmentation is normalized to a rectangular block with the fix polar dimensions using the Daugman's rubber sheet model. The DWT is applied on the normalized Iris image and Lower frequency part of the DWT coefficients, LL, is selected and the mean value of samples is subtracted from all processed Iris Pixels. When the covariance matrix is formed the PCA will be applied on the covariance matrix to obtain the Iris features for recognition. The Euclidean distance is used for classification and obtaining the similarity between the iris templates.

7. Experimental Results and Discussion:

H.K. Rana, et al. [17], have implemented their method, "***Iris Recognition System Using PCA Based on DWT*** "on the CASIA Iris database and their results have been compared with results of other researchers [19-20] as shown in Table 1. They have used Iris images of 40 individuals which have been stored in their own database. Their method is implemented on the entire stored image and the features of each Iris image was obtained and tested against the extracted iris features of other methods in Table-1.

Table 1: Results and Comparison with other Techniques[17].

No.	Methods	Average Recognition Rate
1	DCT feature Extraction Technique based Iris Recognition[19]	75/%
2	DWT feature Extraction Technique based Iris Recognition[19]	82%
3	PCA based recognition[20]	90.2%
4	PCA Based on DWT Feature Selection Technique[17]	92.6%

They have mentioned that, Jyotipoonia, and et al. [19] has applied the DCT and DWT feature extraction technique s on the iris images stored in the CASIA database. Their results of implementation have shown that the average recognition rate for DCT and DWT were75% and 82% respectively. P.S. Patil, et al. [16] also have applied their PCA feature extraction technique on 30 Iris images which their featured already have been stored inside the CASIA database. The average recognition rate for their PCA was 90.2%. The average recognition rate of the methodimplemented by H.K. Rana, et al. [17], was 92.6%. The results indicate the good improvement based on the PAC based on the DWT for the Iris feature selection technique. We have a new proposed technique similar to the PCA based on the DWT feature extraction.

We also have implemented our algorithm for authentication and identification of the individuals based on the extracted features of the face Image for different databases as shown. The analysis of tabulated values in these tables clearly indicated that DWT-SVD had the best performance for the authentication and recognition regarding to high speed operation and good accuracy. However, where the speed is our concerned, such as recognition of various kind of information in real time, DWT-SVD is suggested but when the accuracy is more concerned we can use one the hybrid methods of HT-SVD or MT-SVD.

Sub1Session1-Frame1	Frame1	Frame2	Frame3	Frame4
DWT	0	0.5511	3.3954	9.0238
DCT	0	1.424	8.7743	23.3188
HT	0	0.0206	0.1271	0.3378
MT	0	0.0002	0.0013	0.0034

Fig. 1. Mean Square Errors of 4 Pictures from same Man

Sub1Session1-Frame2	Frame1	Frame2	Frame3	Frame4
DWT	0.5508	0	3.202	8.8985
DCT	1.4185	0	8.2457	22.9152
HT	0.0206	0	0.1199	0.3333
MT	0.0002	0	0.0012	0.0033

Fig. 2-Mean Square Errors of 4 Pictures from same Man

Sub1Session1-Frame3	Frame1	Frame2	Frame3	Frame4
DWT	3.293	3.1067	0	5.5515
DCT	8.0755	7.6187	0	13.6146
HT	0.127	0.1198	0	0.2141
MT	0.0013	0.0012	0	0.0021

Fig. 3-Mean Square Errors of 4 Pictures from same Man

Sub1Session1-Frame4	Frame1	Frame2	Frame3	Frame4
DWT	8.2971	8.1854	5.2633	0
DCT	18.914	18.6595	11.9985	0
HT	0.3367	0.3322	0.2136	0
MT	0.0034	0.0033	0.0021	0

Fig. 4-Mean Square Errors of 4 Pictures from same Man

Sub1Session1-Frame 1-4	Frame1	Frame2	Frame3	Frame4
DWT	31125	30031	33000	36406
DCT	76797	78656	67392	76125
HT	56563	56656	55282	55046
MT	59141	59375	59015	51234

Fig. 5-Process Time (MS) of 4 Pictures from same Man

ISBN: 978-1-941968-59-8 ©2019 SDIWC

8. Conclusions and Future Recommendations:

The Iris image has very rich texture information and this information is randomly oriented in all directions and has multiple frequencies components that need to be considered. Traditional feature extraction and selection techniques are difficult and time consuming due to the large number of features in the Iris texture, especially when these features are statistically independent. To obtain the high resolution feature extraction, a combination of methods and algorithms are required to make sure that all intelligent information in the Iris are captured and extracted for the recognition. Most researchers have used the Gabor filter in which fixed numbers of filter masks are used with predetermined frequencies and bandwidths. The outputs of the Gabor filter banks are non-orthogonal and they will degrade more Iris features in the region of noisy images.

The most important problem in the Iris image recognition is the effects of the CLL on the captured image, the CCL with printed pattern image or the printout of the Iris image. The researchers are familiar with this problem which badly has degraded the captured Iris image and have applied both hardware and software techniques to reduce the effect of CCL. Since the effect of clear soft prescription lenses on recognition accuracy has been understated until recently, the research focus has been on textured contact lens detection and many hardware and software based approaches (and combination of both) have been proposed in the literature. Although the hardware-based solution provides efficient and generalized means for presentation attack detection but due to its additional interaction and limitation it is not the most optimal one and a robust software-based approach that can only work based on the standard Iris sensor would be the best solution for Iris recognition. In addition, the noisy environment can degrade the cyber security recognition system because the effect of noise on the capture Iris image will change the extracted features which are required to be compared with that feature in the database.

Our proposed method is based on the Discrete Wavelet Transform to reduce the effect noise when the Iris and face images are captured in the noisy environment. Once the effects of the noise are reduced then the Singular Value Decomposition should be applied on the DWT output codes to create the singular values which are invariant under rotation and transformation. These singular values are carried the vital information regarding to the faceIris images. Some efficient algorithm should be applied on these singular values to obtain the number of dominant singular values for system order reduction. The dominant singular values of the captures face-Iris images will be compared with the dominate singular values of the Iris image in database. The Support Vector Machine or any type of classifier will be used to perform the recognition process.

The Iris image recognition still has a big challenge regarding to the direct attacks, attacks related cosmetic contact lens CLL with printed patterns, and printout Iris, as well as noisy environment. The advanced technology also gave upper hand to the intruder and hacker to use various types of tricks to deceive the cyber security system and mobile system. We have proposed a new method wich some type of preprocessing algorithm is suggested to remove the effects of the eyelash and eyelid and possibly remove the pupil information in the captured Iris image. Then DWT will be applied on the preprocessed Iris information. We finally have suggested that Singular Value Decomposition Technique (SVD) to be applied on the DWT coefficients and dominated singular values be selected as the feature vector for the comparison process if the speed is our concern otherwise we can use HT-SVD or MT-SVD to get more accurate result for recognition but may be slower.

One way that no one has not worked on it is the recognition of the eye ball of an authorized user with dead body, and high resolution software and hardware need to be developed to recognized the lived Iris image from the fake Iris image, especially when the eye ball of the dead person is presented to the security system for recognition

9. 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] 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.

[3] H. Mehrabian, "Identification of the Identity based on the Iris Signal Analysis", Senior Project, Tehran university, Tehran, Iran, 2015.
[4] 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.
[5]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.
[6] 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.
[7] 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 International
Conference on Biometrics Theory, Applications and Systems (BTAS), pages 1–6, Sept 2015
[8] 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.
[9] 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.
[10] A. F. Sequeira, J. Murari, and J. S. Cardoso, " Iris Liveness Detection Methods in Mobile Applications", https://www.researchgate.net/publication/271516730, May 2014.
[11] 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
[12]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.
[13] 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.
[14] F. Pala, B. Bhanu, "Iris Liveness Detection by Relative Distance Comparisons ", CVPR, 2017.
[15] 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.
[16] 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.
[17] 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. [18] 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.[19]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.
[20]P. S. Patil, S R Kolhe, R V Patil, P M Patil, "The Comparison of Iris Recognition using Principal Component Analysis, Log Gabor and Gabor Wavelets", International Journal of Computer Applications. 2012; 43: 0975 -8887. [21] 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.
[22] 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.
[23] Javier Galbally, A.G.Barrero," A Revie of Iris Anti-Spoofing ", 978-1-4799-8105-2/15, 2016 IEEE.
[24]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.
[25**]** E. Wolff, Anatomy of the eye and orbit, 7th edition. H. K. Lewis & Co. LTD, 1976.
[26]Aertec Solutions, "Biometric Identification at Airports", 27/03/2017, https://www.aertecsolutions.com/2017/03/27/biometric-identification-at-airports/?lang=en.
[27] 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.
[28] 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.