A BIO INSPIRED ALGORITHM FOR BIOMETRIC FAKE DETECTION USING FACE, FINGER & IRIS

***Snehal G.Parate,**
**** Mrs.Pooja Thakre**
** M.Tech Student, department of VLSI,*
Nuva college of Engineering And Technology
Kalmeshwar, Nagpur, India
** Professor, department of Electronics and Telecommunication,
Nuva college of Engineering And Technology
Kalmeshwar, Nagpur, India

ABSTRACT

The biometric person recognition technique based on the pattern of the human iris, face and fingerprint well suited to be applied to access control and provide strong security .A typical biometric system consists of sensing, feature extraction, and matching modules. But now a day's these systems are attacked by using fake biometric. Also the methods used are slow and expensive. To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. There are various search techniques among which Genetic algorithms (GAs) are powerful search techniques that are used successfully to solve problems in many different disciplines .In this paper Genetic algorithm (GA) is used with 25 General Image quality features for biometric fake detection using Face, Fingerprint and Iris. Genetic algorithm does not require special equipment's and can be used in system where fast detection is required. Proposed System, it is a software based system which is used for multiple fake detections with the help of database.

Keywords: Image Quality Assessment, Genetic Algorithm, Liveness Detection, Security, Attacks, Database.

INTRODUCTION

Biometric identification is an automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual. Biometric science utilizes the measurements of a person's behavioral characteristics (keyboard strokes, mouse movement) or biological characteristics (fingerprint, iris, etc). It is these measurements that are then used to create a reference template, which the recognition software uses to identify or authorize an individual as the person they claim to be. Biometric system implementation for person identity verification purposes, terrorist acts prevention measures,

authentication process simplification in computer systems and many other tasks has raised significant attention to reliability and efficiency of biometric systems. Modern biometric systems still face many reliability and efficiency related issues such as reference database search speed, errors while recognizing of biometric information or automating biometric feature extraction. Scientific investigations show that application of evolutionary algorithms may significantly improve biometric systems. That is why it is necessary to get an understanding of evolutionary algorithms and current research done in this area for practical improvement of biometric system quality. Evolutionary algorithms are inspired by Darwinian evolution mechanisms which include reproduction, mutation, recombination and selection. Genetic Algorithms (GA) which are considered to be a part of Evolutionary algorithms, could mimic nature to computationally emulate the same survival of the fittest paradigm for difficult problems. GAs are non-deterministic methods that employ crossover and mutation operators for deriving offsprings. GAs are fully defined when one provides the strategy for deriving the offsprings and the composition of the next generation. Simulated breeding is the usual strategy used when offsprings are selected according to their fitness. GAs work by maintaining a constant-sized population of candidate solutions known as individuals ('chromosomes'). The power of a GA lies in its ability to exploit, in a highly efficient manner, information about a large number of individuals.

Among the different threats analyzed, the so-called *direct*or *spoofing* attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in modalities such as the iris, the fingerprint and the face. In these attacks, the intruder uses some type of synthetically produced artifact (e.g., gummy finger, printed iris image or face mask), or tries to mimic the behavior of the genuine user (e.g., gait, signature), to fraudulently access the biometric system. As this type of attacks are performed in the analog domain and the interaction with the device is done following the regular protocol, the usual digital protection mechanisms (e.g., encryption, digital signature or watermarking) are not effective .The fore mentioned works and other analogue studies, have clearly shown the necessity to propose and develop specific protection methods against this threat. This way researchers have focused on the design of specific counter measures that enable biometric systems to detect fake samples and reject them, improving this way the robustness and security level of the systems .Besides other anti-spoofing approaches such as the use of multi biometrics or challenge-response methods, special attention has been paid by researchers and industry to the *liveness detection* techniques, which use different physiological properties to distinguish between real and fake traits. Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements : *(i)* non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user; *(i i)* user friendly, people should not be reluctant to use it; *(i i i)* fast, results have to be produced in a with the sensor for a long period of time; *(iv)* low cost, a wide use cannot be expected if the cost is excessively high;*(v)* performance, in addition to having a good fake detection rate, the protection scheme should not degrade the recognition performance (i.e., false rejection) of the biometric system. Liveness detection methods[1] are usually classified into one of two groups *(i) Hardware-based* techniques, which add some specific device to the sensor in order to detect particular properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye);*(i i) Software-based* techniques, in this case the fake trait is detected once the

sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake traits are extracted from the biometric sample, and not from the trait itself).The two types of methods present certain advantages and drawbacks over the other and, in general, a combination of both would be the most desirable protection approach to increase the security of biometric systems. As a coarse comparison, hardware-based schemes usually present a higher fake detection rate, while software-based techniques are in general less expensive (as no extra device is needed), and less intrusive since their implementation is transparent to the user. Furthermore, as they operate directly on the acquired sample (and not on the biometric trait itself), software-based techniques may be embedded in the feature extractor module which makes them potentially capable of detecting other types of illegal break-in attempts not necessarily classified as spoofing attacks.

In the present work we propose a novel software-based multi-biometric and multi-attack protection method which targets to overcome part of these limitations through the use of image quality assessment (IQA). It is not only capable of operating with a very good performance under different biometric systems (multi-biometric) and for diverse spoofing scenarios, but it also provides a very good level of protection against certain non-spoofing attacks (multi-attack). Moreover, being software-based, it presents the usual advantages of this type of approaches: fast, as it only needs one image(i.e., the same sample acquired for biometric recognition) to detect whether it is real or fake; non-intrusive; user-friendly(transparent to the user); cheap and easy to embed in already functional systems (as no new piece of hardware is required).An added advantage of the proposed technique is its speed and very low complexity, which makes it very well suited to operate on real scenarios (one of the desired characteristics of this type of methods). As it does not deploy any trait-specific property (e.g., minutiae points, iris position or face detection),the computation load needed for image processing purposes is very reduced, using only *general* image quality measures fast to compute, combined with very simple classifiers

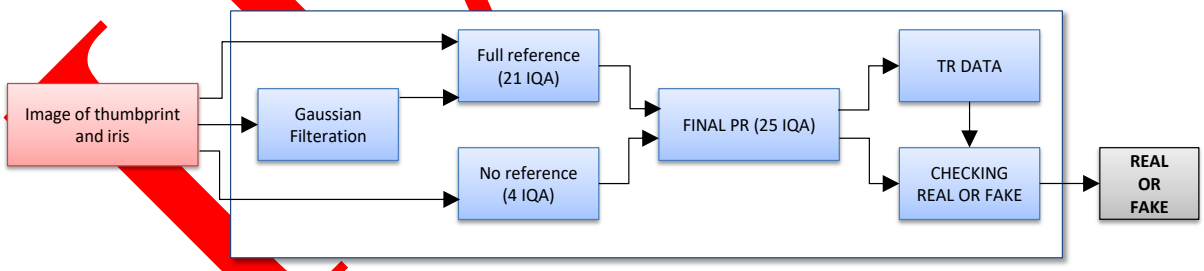

Fig 1.General diagram of the biometric protection method based on I

IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

The use of image quality assessment for liveness detection is motivated by the assumption that: "It is expected that a fake image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario for which the sensor was designed."Expected quality differences between real and fake samples may include: degree of sharpness, color and luminance levels, local artifacts, amount of information found in both type of images (entropy), structural distortions or natural appearance. For example, iris images captured from a printed paper are more

likely to be blurred or out of focus due to trembling; face images captured from a mobile device will probably be over- or under-exposed; and it is not rare that fingerprint images captured from a gummy finger present local acquisition artifacts such as spots and patches. Furthermore, in an eventual attack in which a synthetically produced image is directly injected to the communication channel before the feature extractor, this fake sample will most likely lack some of the properties found in natural images. Following this "*quality-difference*" hypothesis, in the present research work we explore the potential of *general* image quality assessment as a protection method against different biometric attacks (with special attention to spoofing).

As the implemented features do not evaluate any specific property of a given biometric modality or of a specific attack, they may be computed on any image. This gives the proposed method a new multi-biometric dimension which is not found in previously described protection schemes. In the current state-of-the-art, the rationale behind the use of IQA features for liveness detection is supported by three factors: • Image quality has been successfully used in previous works for image manipulation detection and steg analysis in the forensic field. To a certain extent, many spoofing attacks, especially those which involve taking a picture of a facial image displayed in a2D device (e.g., spoofing attacks with printed iris or face images), may be regarded as a type of image manipulation which can be effectively detected, as shown in the present research work, by the use of different quality features.• In addition to the previous studies in the forensic area, different features measuring trait-specific quality properties have already been used for liveness detection purposes in fingerprint and iris applications .

However, even though these two works give a solid basis to the use of image quality as a protection method in biometric systems, none of them is general. For instance, measuring the ridge and valley frequency may be a good parameter to detect certain fingerprint spoofs, but it cannot be used in iris liveness detection. The problem of fake biometric detection can be seen as a two-class classification problem where an input biometric sample has to be assigned to one of two classes: real or fake. The key point of the process is to find a set of discriminate features which permits to build an appropriate classifier which gives the probability of the image "realism" given the extracted set of features. In the present work we propose a novel parameterization using 25 general image quality measures [1]. A general diagram of the protection approach proposed in this work is shown. In order to keep its generality and simplicity, the system needs only one input: the biometric sample to be classified as real or fake (i.e., the same image acquired for biometric recognition purposes). Furthermore, as the method operates on the whole image without searching for any trait-specific properties, it does not require any pre processing steps (e.g., fingerprint segmentation, iris detection or face extraction) prior to the computation of the IQ features. This characteristic minimizes its computational load. Once the feature vector has been generated the sample is classified as real (generated by a genuine trait) or fake (synthetically produced), using some simple classifiers.

The parameterization proposed in the present work comprises of 25 image quality measures both reference and blind. As it would be unfeasible to cover all the immense range of methods, approaches and perspectives proposed in the literature for IQA, the initial feature selection process to determine the set of 25 IQMs has been carried out according to four general criteria, which intend that the final

method complies to the highest possible extent with the desirable requirements set for liveness detection systems (described in Section I). These four selection criteria are:•

Performance. Only widely used image quality approaches which have been consistently tested showing good performance for different applications have been considered.•

Complementarity. In order to generate a system as general as possible in terms of attacks detected and biometric modalities supported, we have given priority to IQMs based on complementary properties of the image(e.g., sharpness, entropy or structure).•

Complexity. In order to keep the simplicity of the method, low complexity features have been preferred over those which require a high computational load.•

Speed. This is, in general, closely related to the previous criterion (complexity). To assure a user-friendly non-intrusive application, users should not be kept waiting for a response from the recognition system. For this reason, big importance has been given to the feature extraction time, which has a very big impact in the overall speed of the fake detection algorithm.

a) Face recognition and attack on system

The most acceptable biometrics is Face reorganization, because it is one of the most universal methods of identification that humans use in their visual interactions and acquisition of faces [7]. The face recognition systems make different between the background and the face. It is most important when the system has to identify a face within a throng. The system then makes use of a person's facial features – its valleys and peaks and landmarks and treats these as nodes that can be compared and measured against those which are stored in the system's database

b) Fingerprint recognition and attacks on system

Every fingerprint of each person is considered to be unique, Even the Twins also contain different fingerprint. Fingerprint recognition is the most accepted biometric recognition method. Fingerprints have been used from long time for identifying individuals. Fingerprints consist of ridges and furrows on the surface of a fingertip. Now fingerprint recognition system is used in iPhone, there are many areas where the fingerprint recognition system used. But attackers attack on fingerprint recognition system. Attackers first capture real fingerprint then they make fake fingerprint by using silicon, playdoh and gelatin and try to access the system.

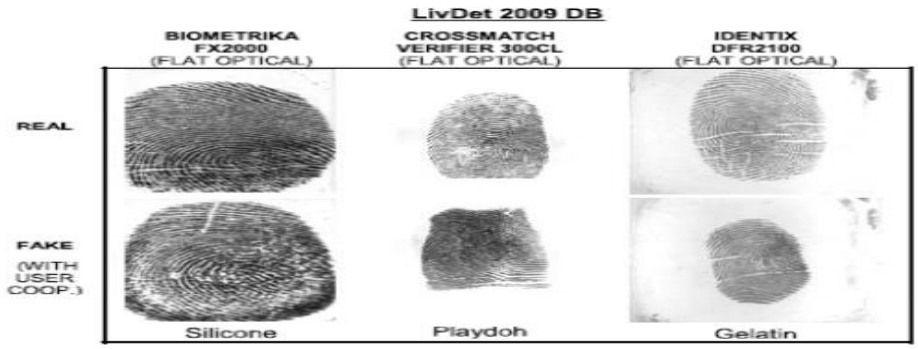

Fig2 Real and fake fingerprint

c) Iris Recognition attacks on system

Iris recognition is a computerized method of biometric identification which uses mathematical Model recognition techniques on video images of the irises of an individual's eyes, whose Complex random patterns are single and can be seen from some distance. Iris cameras perform detection of a person's identity. The iris scans process start to get something on film. It combines computer vision, statistical inference, pattern recognition and optics. The iris is the colored ring around the pupil of every human being and like a snowflake; no two are the same [6]. Each one is unique. An attack on the iris is not so easy but how to attack on the system is as shown below. To create a fake iris is of tree

1) Original images are capture for a better quality, then

2) They are printed on a paper using a commercial printer

3) Printed images are presented at the iris sensor

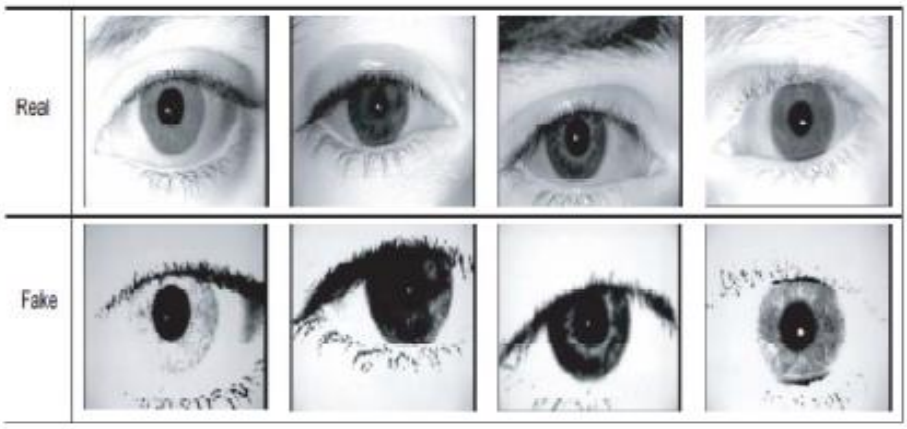

fig3 Fake and real iris

#	Type	Acronym	Name
1	FR	MSE	Mean Squared Error
2	FR	PSNR	Peak Signal to Noise Ratio
3	FR	SNR	Signal to Noise Ratio
4	FR	SC	Structural Content
5	FR	MD	Maximum Difference
6	FR	AD	Average Difference
7	FR	NAE	Normalized Absolute Error
8	FR	RAMD	R-Averaged MD
9	FR	LMSE	Laplacian MSE
10	FR	NXC	Normalized Cross-Correlation
11	FR	MAS	Mean Angle Similarity
12	FR	MAMS	Mean Angle Magnitude Similarity
13	FR	TED	Total Edge Difference
14	FR	TCD	Total Corner Difference
15	FR	SME	Spectral Magnitude Error
16	FR	SPE	Spectral Phase Error
17	FR	GME	Gradient Magnitude Error
18	FR	GPE	Gradient Phase Error
19	FR	SSIM	Structural Similarity Index
20	FR	VIF	Visual Information Fidelity
21	FR	RRED	Reduced Ref. Entropic Difference
22	NR	JQI	JPEG Quality Index
23	NR	HLFI	High-Low Frequency Index
24	NR	BIQI	Blind Image Quality Index
25	NR	NIQE	Naturalness Image Quality Estimator

list of 25 general IQM classification parameters

1) The basic Biometric system is divided into two parts
   a) Training
   b) Testing.

a) Training:

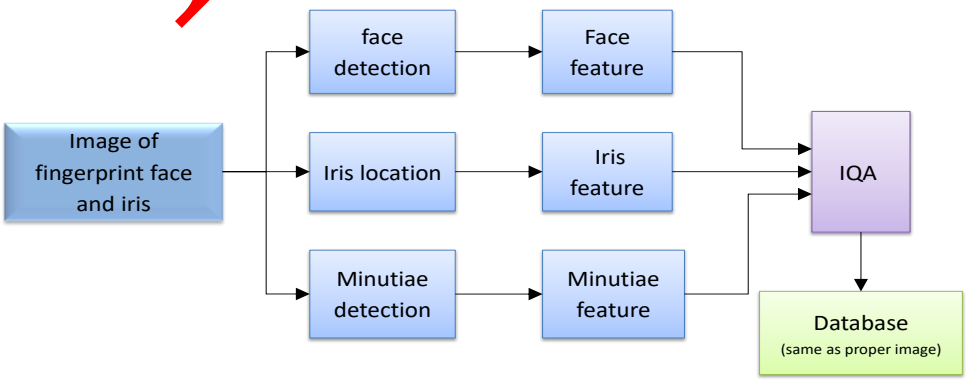

Fig4 training

1. Browse Finger print image.
2. Extract the Minutiae features(by using this user gets the information about the image)
3. Browse Iris image.
4. Extract the Iris features(by using this user gets the information about the image)
5. Browse Facial image.
6. Extract the Facial features(by using this user gets the information about the image)
7. All the features of Minutiae, Iris and Face will be forwarded to IQA ie Image Quality Assessment where these features will be classified on the basis of 25 Image Quality Measures.
8. The output of IQA will then be saved into Database for further reference.

b) Testing:

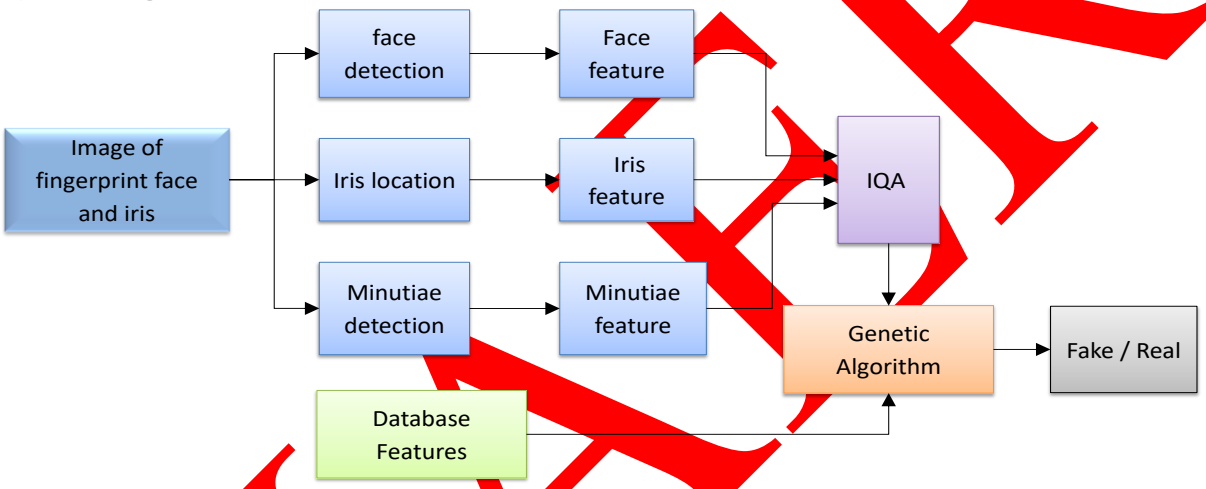

Fig5 testing

1. Browse Finger print, Iris and Facial images individually.
2. Extract all the features of Minutiae, Iris and Facial images(by using this user gets the information about the image)
3. All the features of Minutiae, Iris and Face will be forwarded to IQA i.e. Image Quality Assessment where these features will be classified on the basis of 25 Image Quality Measures.
4. The output of IQA will be forwarded to Genetic Algorithm (search algorithm) where all these features of images will be compared with the Database images (stored during training process).
5. Genetic algorithm will search for the most possible match (saved as real image in database) and filter out the fake images.

GENETIC ALGORITHM

The genetic algorithm is a search heuristic that mimics the process of natural evolution. This heuristic is routinely used to generate useful solutions to optimization and search problems. Genetic algorithms belong to the larger class of Evolutionary Algorithms (EA), which generate solutions to

optimization problems using techniques inspired by natural evolution, such as inheritance, mutation, selection and crossover. In a genetic algorithm, a population of strings (called chromosomes or the genotype of the genome), which encode candidate solutions (called individuals, creatures or phenotypes) to an optimization problem, evolves toward better solutions [5][6]. Traditionally, solutions are represented in binary as strings of 0s and 1s, but other encodings are also possible. The evolution usually starts from a population of randomly generated individuals and happens in generations. In each generation, the fitness of every individual in the population is evaluated, multiple individuals are stochastically selected from the current population (based on their fitness), and modified (recombined and possibly randomly mutated) to form a new population. The new population is then used in the next iteration of the algorithm. Commonly, the algorithm terminates when either a maximum number of generations has been produced, or a satisfactory fitness level has been reached for the population. If the algorithm has terminated due to a maximum number of generations, a satisfactory solution may or may not have been reached. The typical genetic algorithm requires a genetic representation of the solution domain and a fitness function to evaluate the solution domain. The genetic algorithm is a model of machine learning which derives its behaviour from a metaphor of some of the mechanisms of evolution in nature. This is done by the creation within a machine of a population of individuals represented by chromosomes, in essence a set of 81 character strings that are analogous to the base-4 chromosomes. The individuals represent candidate solutions to the optimization problem being solved. In genetic algorithms, the individuals are typically represented by n-bit binary vectors. The resulting search space corresponds to an n dimensional boolean space (Oliveira et al. 2002). It is assumed that the quality of each candidate solution can be evaluated using a fitness function as shown. A standard representation of the solution is as an array of bits. Arrays of other types and structures can be used in essentially the same way.

The main property that makes these genetic representations convenient is that their parts are easily aligned due to their fixed size, which facilitates simple crossover operations. Variable length representations may also be used, but crossover implementation is more complex in this case. Tree-like representations are explored in genetic programming and graph-form representations are explored in evolutionary programming. The fitness function is defined over the genetic representation and measures the quality of the represented solution. The fitness function is always problem dependent. For instance, in the knapsack problem one wants to maximize the total value of objects that can be put in a knapsack of some fixed capacity. A representation of a solution might be an array of bits, where each bit represents a different object, and the value of the bit 0 or 1 represents whether or not the object is in the knapsack. Not every such representation is valid, as the size of objects may exceed the capacity of the knapsack. The fitness of the solution is the sum of values of all objects in the knapsack if the representation is valid or 0 otherwise. In some problems, it is hard or even impossible to define the fitness expression, in these cases interactive genetic algorithms are used. Once the use of genetic representation and the fitness function defined, genetic algorithm proceeds to initialize a population of solutions randomly and then improve it through repetitive application of initialization, mutation, crossover and inversion and selection operators. Simple generational genetic algorithm pseudo code:

a. Choose the initial population of individuals.

b. Evaluate the fitness of each individual in that population

c. Repeat on this generation until termination: (time limit, sufficient fitness achieved, etc.)

Steps of Genetic algorithm:

i. Select the best fit individuals for reproduction
ii. Breed new individuals through crossover and mutation operations to give birth to offspring
iii. Evaluate the individual fitness of new individuals
iv. Replace least-fit population with new individuals.

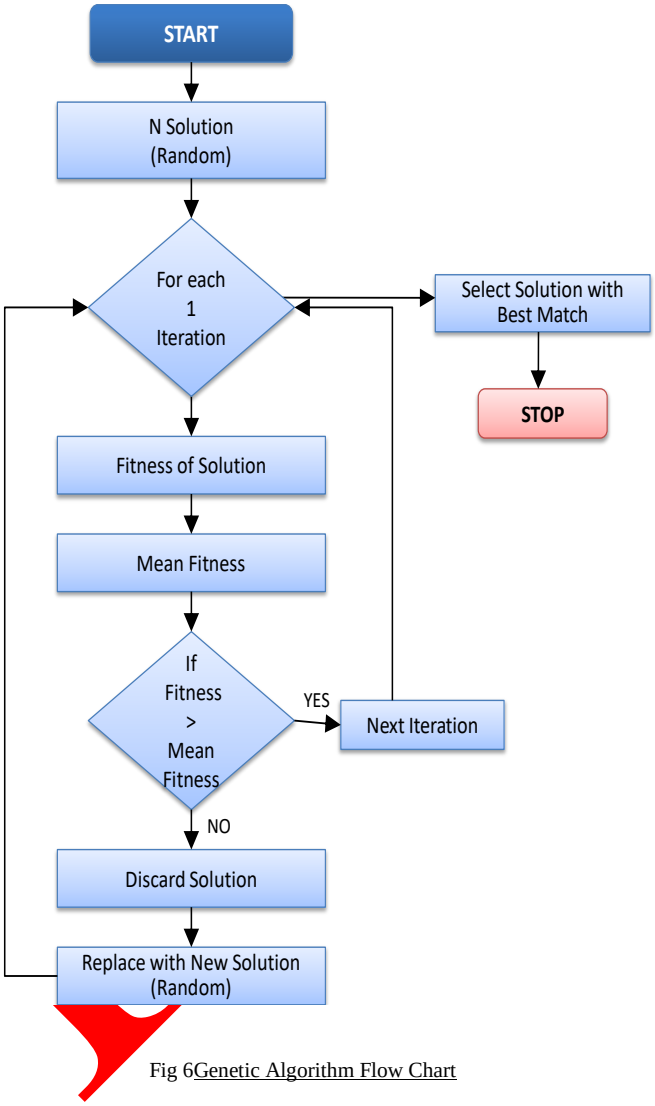

Fig 6Genetic Algorithm Flow Chart

The first component for a genetic algorithm is a binary representation of a solution candidate, in this cases any numeric parameter vector. In analogy to nature vector components are referred to as *genes* and vector representations as *chromosomes*. The *population* of a genetic algorithm is a set of such solution candidates, called *individuals*, which are initialized with random values. A so-called *fitness function* calculates the quality of an individual as a numeric value by determining its conformance to the user specified conditions. The actual optimization is accomplished by an iterative reproduction process. In the first step a small set of individuals with higher fitness values is selected from the

current population. Using these solution candidates a new generation will be created through genetic operators. Mutation operators randomly change single or multiple values in the chromosome, therefore providing a wide exploration of the search space. Crossover mechanisms exchange genes between two or more parent chromosomes to create new individuals. This way with a good chance two potentially good partial solutions are combined. The inheritance of genes that have a positive influence on the solution quality and the preferred selection of individuals with higher fitness values results in a slowly rising average fitness in the population by iteration of the reproduction process. The selection and reproduction cycle is repeated until a user specified termination condition is reached, such as a solution is found that satisfies the target criteria.

RESULT

a)Face Recognition:

Face recognition is a biometric modalities used to determine the identity of the individual which uses the computer software. Face recognition is mainly performed by two approaches i.e, Eigen based face recognition and 3D face recognition. The Eigen face based recognition works by analyzing face images and computing Eigen faces which are faces composed of Eigen vectors. The comparison of Eigen faces is used to identify the presence of a face and its identity. The Eigen face technique is a easy, well-organized, and gives generally better results in controlled environment. Some of the demerits of Eigen faces are robustness to changes in lighting, distance and angle.

Fig 7Typical examples of real and fake (print, mobile and highdef) face images that can be found in the public REPLAY-ATTACK DB used in the face anti-spoofing experiments.

The performance of the IQA-based protection method has also been assessed on a face spoofing database: the REPLAY-ATTACK DB [57] which is publicly available from the IDIAP Research Institute.

b)Fingerprint recognition:

A fingerprint is the made of ridges and valleys on the surface of a fingertip. The fingerprints are highly stable and unique. The uniqueness of fingerprint is determined by the prototype like valleys and ridges, as well as minutiae points which are local ridge characteristics that occurs at either a ridge bifurcation or ridge endings. The recent studies shows that probability of two individuals fingerprint, having the same fingerprint is less than one in a billion. There are several fingerprint matching algorithms like minutiae based matching, correlation based matching, genetic algorithms based matching. Among these algorithm, minutiae based matching is the best one. In minutiae based matching the similarity of two fingerprints is determined by computing the total number of matching minutiae i.e. ridges and valleys from these two scanned fingerprints. Extraction of minutiae features before matching fingerprint requires a series of processes containing position calculation, image segmentation, image enhancement, and ridge extraction and shinning, minutiae. Extraction and filtering,

Results: Fingerprints-Spoofing LivDet: The LivDet2009 DB [10] was captured in the framework of the 2009Fingerprint Liveness Detection Competition and it is distributed through the site of the competition.4 It comprises three datasets of real and fake fingerprints captured each of them with a different flat optical sensor: *i*) BiometrikaFX2000 (569 dpi), *i i*) Cross Match Verifier 300CL (500 dpi),and *i i i*) Ident ix DFR2100 (686dpi). The gummy fingers were generated using three different materials: silicone, gelatine and playdoh, always following a consensual procedure (with the cooperation of the user).

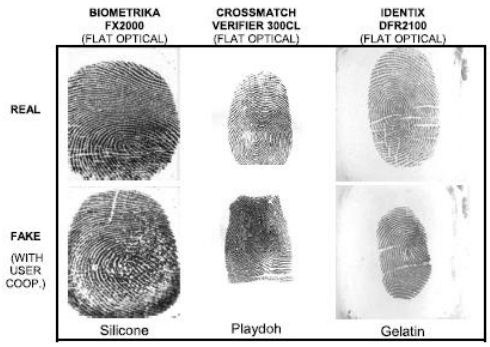

Fig8 Typical examples of real and fake fingerprint images that can be found in the public LivDet09 database used in the fingerprint anti-spoofing experiments.

c) Iris recognition:

Iris recognition systems make use of the uniqueness of the iris patterns to identify a person. This system uses high quality camera to capture a black-and-white image, high resolution image of the iris. Iris is the colored ring surrounding the pupil. Iris recognition consists of five operations; they are image acquisition, iris localization or segmentation, iris normalization and unwrapping, feature

encoding, and matching algorithm. In image acquisition step the systems takes a high-quality image of the iris, Iris localization takes place to detect the edge of the iris as well as that of the pupil; thus extracting the iris region, Normalization is used to transform the iris region to have fixed dimensions, and hence removing the dimensional inconsistencies between eye images, other inconsistencies include varying image distance, camera rotation, eye rotation within eye socket, tilting of the head, the normalized iris region is unwrapped into a rectangular region.

Results: Iris-Synthetic: During this situation attacks area unit per-formed with synthetically generated iris samples that area unit injected within the communicating between the detector and also the feature extraction module. The important and pretend databases utilized in this case are: • Real database: CASIA-IrisV1.This dataset is publical layout there through the Biometric Ideal take a look at (BIT) platform of the Chinese Academy of Sciences Institute of Automation (CASIA).2 It contains seven grey-scale 320×280 pictures of 108 eyes captured in 2 separate sessions with a self-developed CASIA close-up camera and area unit hold on in bmp format. • Artificial database: WVU-Synthetic Iris decibel. Being a info that contains solely absolutely artificial information, it's not subjected to any legal constraints and is publically out there through the CITER centre.3The artificial irises area unit generated following the tactic delineated, that has 2 stages. Within the first stage, a Markoff Random Field model trained on the CASIA-IrisV1 decibel is employed to get a background texture representing the world iris look.

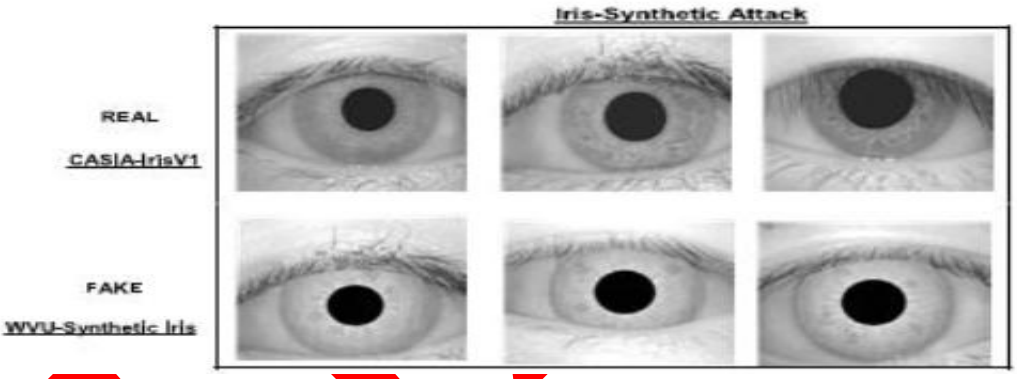

fig 9 .Typical real iris images from CASIA-IrisV1 and fake samples from WVU-Synthetic Iris

A consequence of the coaching method administered on the CASIA-IrisV1 decibel, the artificial samples area unit visually terribly almost like those of the important dataset, that makes them specially appropriate for the thought of assaultive situation. The last column indicates, in seconds, the typical execution time to method every sample. In the experiments, so as to possess balanced coaching categories (real and fake) solely fifty four artificial eyes were willy-nilly elect. This way, the matter of overfitting one category over the opposite is avoided.

CONCLUSION

The study of the vulnerabilities of biometric systems against different kinds of attacks has been awfully active field of analysis in recent years. This interest has cause massive advances within the field of security-enhancing technologies for biometric-based applications. For this purpose a feature space of 25 complementary image quality measures are considered which are combined with genetic

algorithm to detect real and fake access attempts. The novel protection method has been evaluated on three largely deployed biometric modalities such as the iris, the fingerprint and 2D face. Here genetic algorithm improves speed and accuracy of biometric system.

REFERENCES

1. Javier Galbally, Sébastien Marcel, and Julian Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition" IEEE transactions on image processing, vol. 23, no. 2, February 2014.
2. N. Goranin and A. Cenys "Evolutionary Algorithms Application Analysis in Biometric Systems" Journal of Engineering Science and Technology Review 3 (1) (2010) 70-79.
3. Mrinmoyee Bhattacharya, ShashiKala.D, M.N.Nachappa, Mary Merline "Genetic Algorithm And Its Application In Biometric Authenticating System" JECET; June 2014-August 2014; Sec. B Vol.3.No.3, 1436-1444
4. R. Radhika, D. Sanjana, C. Anuradha "Fake Biometric Detection to Iris, Fingerprint Using Image Quality Assessment" International Journal of Advanced Research in Computer Science and Software Engineering.
5. Pratibha P. Chavan, Dr. M Murugan, Pramod U. Chavan "Genetic Algorithm based Feature Subset Selection in Face Detection" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
6. Xuejun Tan, Bir Bhanu "Fingerprint matching by genetic algorithms" Pattern Recognition 39 (2006) 465 – 477
7. Pradnya M. Shende, Dr.Milind V. Sarode, Prof. Mangesh M. Ghonge "A Survey Based on Fingerprint, Face and Iris Biometric Recognition System, Image Quality Assessment and Fake Biometric" International Journal of Computer Science Engineering and Technology(IJCSET)
8. Ms. Kavita H. Waghmode, Dr. Prof. P.K. Ajmera "Image Quality Assessment For Fake Biometric Detection: Application To Iris, Fingerprint, And Face Recognition" IJIERT ISSN: 2394-3696.
9. Mukesh Rinwa, Bharat Borkar International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064
10. Shalin Shaji K, Biju H, Arun Basker Image Quality Assessment for Multimodal Fake Biometric Detection: A survey" International Journal of Advanced Research Trends in Engineering and Technology.