TECHNOLOGIES TO OVERCOME SPOOFING ATTACK IN FACIAL RECOGNITION

Kriti Pratap, Anjali Priya, Gayathri Mani

Abstract: *The identification technologies used nowadays consists of biometrics as an essential component. The basic use of a conventional biometric system is to identify the authenticity of an individual through its physical as well as behavioral attributes, which is considered as one of the most suitable method to secure confidentiality of data. Though the security of these systems is stringent to breach, still it does consists of vulnerabilities due to various reasons. One of the major threats the current biometric system possess are the spoofing attacks. Spoofing attacks are difficult to conquer due to the fact that a person tries to masquerade as others in order to gain unauthorized access to the security systems. This is one of the biggest problem concerning the integrity of the biometric system. The study of spoofing attacks has gained interest of various researchers in the field of computer science, still there are aspects which needs greater attention in order to achieve a plausible solution. The study is based on the current biometric systems in order to compare and contrast the existing technology used in facial recognition. A detailed review of the existing anti – spoofing methods will be taken into account to discuss the future research directions. Thus, the work will focus on threats to the current security systems, with an aim to analyse the possible countermeasures, and its applications in real life scenarios.*

Keywords: *Biometrics, Face Recognition, Security, Spoofing Attack, Vulnerability, Machine Learning.*

I. INTRODUCTION

Security of personal data is a major concern in recent times, and to ensure that only authorized person have access to data is even more important. Though due to advancement in technology, highly secure passwords can be created in order to secure critical data, still it puts the risk as they can often by cracked by attackers. A complex password might offer improved security, but it comes with cost of difficulty in remembering and storing these passwords. If same password is being used in multiple platforms, it puts the user in risk of access to multiple resources in case of security breach.

An effective alternative to these methods is to secure critical data by user's biological characteristics. These include one or combination of features which includes their face, fingerprint, iris, voice and hand geometry [11]. These offer much better levels of security as they cannot be easily stolen or lost. Though, these biometric system possess better levels of security than password, these too are prone to various attacks. These might include attacks such as impersonating the authentic user by attacker, known as spoofing attack, or even using external methods such as videos or masks in case of facial authentication to resemble the identity of a legitimate user.

Revised Manuscript Received on July 05, 2019.

Kriti Pratap, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India
Anjali Priya, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India
Gayathri Mani, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India

This study highlights the common threats that a biometric system possesses along with the researched review of current anti-spoofing techniques [19] in practice. The purpose of this research is to analyse both, spoofing attacks and its countermeasures in the biometric system. This study in particular, focuses on the facial recognition biometric system, with a purpose to provide a brief overview of development in this field. This further highlights the research directions that concerned authorities seek in order to minimize the attacks on the biometric systems.

.

II. BIOMETRICS

Biometrics is the statistical analysis and measurement of unique physical and biological characteristics of people. This technique is used to secure entry, data or access using human biological information. These biometrics that is commonly used include fingerprint, iris, face, voice and numerous emerging modals such as gait, and ear. Each of this has its own strengths and weakness which can be exploited for its applications.

Biometric system function in two modes, authentication and identification. Authentication is used to confirm the identity, while identification aims to recognize a particular individual. These two modes have basic operation of feature – to – reference comparison.

Biometrics is the statistical analysis and measurement of unique physical and biological characteristics of people. This technique is used to secure entry, data or access using human biological information. These biometrics that is commonly used include fingerprint, iris, face, voice and numerous emerging modals such as gait, and ear. Each of this has its own strengths and weakness which can be exploited for its applications.

Biometric system function in two modes, authentication and identification. Authentication is used to confirm the identity, while identification aims to recognize a particular individual. These two modes have basic operation of feature – to – reference comparison.

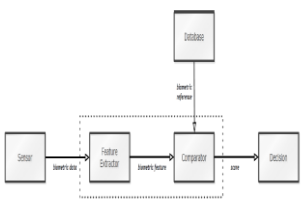

Figure 1: A biometric system

The data when acquired from the sensors, is compared to the existing samples present in the system. If the identity

matches, it is identified as an authentic login based on its features.

One of the most basic biometric authentication system used is facial recognition, which is used to identify a legitimate user. It is a biometric authentication application that verifies a person by analyzing facial contours. These system function based on different nodal points on face, and the data captured can quickly identify the individual. Though being highly useful, it is prone to numerous attacks such as spoofing attack and presentation attack.

III. SPOOFING ATTACK

The biometric system are prone to numerous attacks, which can be categorized into two categories, *direct* and *indirect* [11]. Direct attacks are active at the sensor level, not within the limits of a biometric system. While the indirect attack is within the computed limits by the attacker [11]. These bypass the feature extractor to exploit the vulnerabilities in communication channel.

Direct attack such as *spoofing attack* or *presentation attack* a significant concern while considering the security of the system. These cannot be prevented through traditional digital protection methods as in case of indirect attacks. Thus a typical intruder can bypass the security by impersonating as an authentic user. A biometric system must be capable of accepting the genuine users and rejecting the imposters through a significant verification method.

The spoofing attacks can be detected using numerous methods. The basic countermeasures include liveness detection which aims to detect the signs of life. A multi-modal system can also be deployed to detect the user based on multiple modalities. Though the countermeasures for the spoofing attacks is still under research, few attempts have been made to increase the reliability of biometric systems.

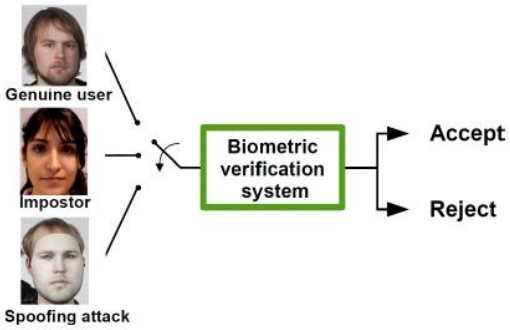

Figure 2: Verification process in a Biometric system.

IV. CASE STUDY

4.1 Face Spoofing Detection using Image Distortion Analysis

Using of Automatic Face Recognition in day to day life has raised the concern governing the integrity of facial biometric systems. An efficient and robust mechanism Image Distortion Analysis is an algorithm to tackle face spoofing attacks. The IDA algorithm comprises of the following:

1. A mechanism capable of gathering innate disfigurements of spoof face in comparison to the original face.
2. A face spoof database called as MSU Mobile Face Spoof Database which uses the cameras of laptops and mobile phones and any three types of attack medium to evaluate the deduction of face spoofing algorithms.

4.1.1 Features Extracted from IDA

The mobile phones that detect the face spoofing attack make the decision based on instant realtime data that consists of numerous frames which can be extended up to 30 frames. Thus, while evaluating the single frames, it is important to infer features capable of finding a distinction between an original face and a spoofed face.

A. Specular Reflection Features: Specular Reflection components are required in elimination of specular reflection [1] and face illumination normalization, in a large range. It involves the separation of specular reflection component, using an iterative method which assumes, illumination is from a single source of stable color without being oversaturated.

B. Blurriness Features: Spoofing is involved in a limited range due to the fact that the external user needs to place the camera in closeness to the boundary of the medium [1].This results in the spoof faces being de-focused which can act as prompt for anti-spoofing [1]. The difference between the original image and the blurred image gives the measurement of blurriness [1]. Another method to measure the blurriness is by measuring the average edge width from the input image [1].

C. Chromatic Moment Features: There is always a difference between the recaptured images and the original images created by the improper color generative property of display and printed media. The RGB space is converted into HSV (Hue, Saturation and Value) space and then calculate the mean, deviation and skewness of each channel.

D. Color Diversity Features: The original images have richer colors in comparison to the spoofed images which arises the condition for color diversity. It involves the quantization of colors on normalized face images then two measurements are added from the distributed colors: i) the histogram bin count of uppermost 100 occurring color , and ii) the number of well-defined colors that appear.

4.2. Presentation Attack Detection

Most of the imaging systems are dependent on the usage of real world information by converting it to a 2D image which works for a known amount of visioning where the device is capable of resolving information to a limited amount [2]. A particular plane is focused for a specific focal

length and aperture, and all other planes are gone unnoticed. Here comes the need to use light field imaging where the entire scene information is captured rather than one single plane.

4.2.1 PAD Scheme

This section comprises of the PAD scheme using Lyro light field camera [2]. The camera has the unique quality of capturing the face image with multiple focus images such that each image will have only one particular depth region in focus [2].

A. *Face Detection and Pre-Processing*: In order to remove number of false positives, a light field image with multiple number of depth images is evaluated for face-detection and pre-processing which are performed separately.
Face detection is carried using Viola-Jones algorithm [2] where the distance is kept between 1.5 m - 2 m and the face detector is made efficient to detect a face [2]. The next step involves pre-processing of the images using 1) Gaussian filter to remove the noise 2) Resizing operation on the filtered image to get a size of 120x120 in order to reduce cost of data processing [2].

B. *Focus Measure*: Each of the depth image is measured quantitatively using the following four groups (1) Gradient based method: This involves measuring degree of focus using the first derivative of the image. (2) Static based method: This evaluates the degree of focus using image statistics as texture descriptors. (3) Transformation based method: The measurement of degree of focus is implemented Laplacian and wavelets. 4) Image Characteristics based method: This involves measuring sharpness and contrast to measure degree of focus.

C. *Baseline Face Recognition System*: Gabor transform and Space Representation Classifier are combined together for evaluation. There are two ways of combining information form these depth images [2] (1) All-in-focus image construction. (2) Selection of the best focus image based on highest energy. The better result is yielded by the second one thus, in majority of cases Selection of the best focus is used in combination with Gabor Transform to obtain the comparison score.

4.3 Color Texture Analysis for Spoofing Detection

It has been found that counterfeit faces of high resolution are almost impossible to detect using only luminosity information of webcam quality images. Fortunately, the color multiplication of spoofed images are less in comparison to the genuine images. Color Texture Analysis is a technique using different texture descriptors fusion together to get a complementary benefit.

4.3.1 CTA Scheme

The CTA can be operated on a discrete video frame or a number of different video sequences in order to achieve practical real time response.

A. *Color Space:* Due to high interdependence between the three colors (red, green and blue), the utility of RGB gets restricted which results in the erroneous separation of radiant and chrominance information. In this scenario, the other two color spaces HSV and YCbCr are also taken into consideration. In HSV, the chrominance of the image are determined by the tone and saturation dimensions while the luminance is determined by the value of dimensions. In YCbCr [3][13], the RGB components are separated into luminance (Y), chrominance blue (Cb) and chrominance red (Cr). HSV and YCbCr are responsible for providing complementary facial color texture descriptors.

B. *Texture Descriptors:* The color texture of face images is analysed using the given five textures [3][14][16]: Local Binary Patterns (LBP), Co-occurrence of Adjacent Local Binary Patterns (CoALBP), Local Phase Quantization (LPQ), Binarized Statistical Image Features (BSIF) and Scale-Invariant Descriptor (SID) [3][16].

There descriptions are given as follows:

LBP: It is a highly discriminative grey scale texture descriptor. For each pixel in an image a binary code is computed using a threshold circular symmetric neighbourhood with the value of the central pixel.
CoALBP: The packing of LBP patterns are such that it tends to discard the spatial information between the patterns. The end histogram obtained is reshaped to form a final vector feature.
LPQ: This is used to deal with the blurred images.
BSIF: The BSIF descriptor is responsible for computing binary code string for each pixel in an image where each bit is obtained by convolving the image using a linear filter and then binarizing the responses obtained.
SID: It uses the shift property of the Fourier Transform i.e its magnitude is invariant to translations.

4.3.2 Database

A. *CASIA Face Anti Spoofing-Database (CASIA-FASD):* It consists of video recording of original and false faces. Using these three fake face attacks were designed as follows [3]: warped photo attacks, cut photo attacks and video attacks [3].

B. *Replay Database Attacks:* It consists video recordings of real accesses and attack attempts under two illumination conditions [14]: controlled i.e uniform illumination and un-controlled i.e non-uniform illumination. The recordings obtained from replay attacks are used to generate the fake face attacks.

C. *MSU Mobile Face Spoof Database (MSU MFSD):* The

MSU MFSD consists of 280 video recordings of real and fake faces [14]. These recordings are taken using two different cameras. Each subject is made to do two recordings from the different cameras respectively. The final database obtained are divided into two subsets namely, training and testing.

4.4 Face Liveness Detection using Diffusion Speed Model

The exposition features of fake and genuine faces are always distinct. It can be easily inferred that the light on the face is random due to 3-D structure whereas on the fake 2-D image it is uniform [4]. This concludes that illumination growth on a 2-D plane are uniformly dispensed and thus, diffuses at a lower rate. This arises the need to use Diffusion Speed Model [4] to analyse to distinguish between pixel values of original and the fake images [4].

4.4.1 Local Speed Patterns

The principal characteristics of LSP-based [4] Face Representation FLSP are given below:

1. The attention is given more on diffusion speed instead of diffusion result.
2. LSP based feature vector captures the energization factors on the respective platforms. Thus it enhances the robustness of the system and enables it to fight against a number of spoofing attacks across various media.
3. LSP based feature is capable of implementing indoor as well as outdoor since, the model is works reliably under all lighting conditions.
4. The scheme is capable of being implemented in real time scenarios such as mobile devices.

4.4.2 Datasets

A. NUAA: This is the most widely used dataset for evaluating face liveness detection. In this the subjects are made to look at a web-cam with a neutral expression along with some movement such as eye blinking. The fake examples are created using a usual camera and is printed on a photographic paper. It is mandatory to note that there is no overlapping of training and test sets in these datasets.

B. SFL: A smartphone is used to construct a dataset in SFL under varying illumination conditions. The faces of the subjects are captured using full HD camera located on the front side of the smartphone in indoor and outdoor environments. The fake images are obtained by two mechanisms, first is by using another smartphone and the other one is by getting the image on a photographic sheet and then clicking an image out of it.

C. Replay Attack: This dataset generally comprises of 1300 videos, each with a resolution of 320x240 pixels, under different lighting conditions. Each video is captured using two styles one is in fixed position and the other one in hand held position. This dataset is further disintegrated into three subsets comprising of training, development and testing. Replay attacks are capable of being implemented into video based anti-spoofing attacks.

4.5 Machine Learning in Face Recognition

Machine Learning [17] is a revolutionary technique that is continuously bringing change to the world. The broad uses of the ML algorithms in day to day life has made it vulnerable to attacks. As human dependence on machines is increasing day by day, the concern governing the integrity of privacy is also on rise.

4.5.1 Threat Model

It is assumed that an attacker who has gain access to a face recognition system upon the training of the system [5] i.e. the situation is only capable of altering composition of inputs and not the training data. Our focus lies on the adversaries who are aware of the feature space, since feature space are always supposed to be publicly known.

4.5.2 Deceiving Neural Networks

DNNs have proved to work excellent in case of huge set of training data sets and are capable of achieving state-of-the-art results [17] on many ML algorithms [5]. Even after such robustness DNNs are often misled by mild perturbing inputs.

4.5.3 White-box DNNs

It comprises of using three DNNs: DNNA, DNNB and DNNc.

1. DNNA: It was developed by Parkhi et al. to recognise 2622 celebrities using 1000 images roughly for each celebrity, still achieving 98.95% accuracy.
2. DNNB and DNNC: Since, DNNA was not trained to identify users available for testing physical attacks thus, arise the need to use DNNB and DNNC.

DNNB was trained to recognise ten subjects while DNNC was trained to recognise a greater set of users. These two methods were trained using transfer-learning procedure. The initial set of layers are copied from the current DNN with the addition of new layers to the old ones and the new parameters are being trained for the new task. DNNB gained classification accuracy of 97.43% [17], and DNNC gained accuracy of 96.75% [17].

4.5 Liveness Detection using Flash

The recognition of face is vulnerable to numerous attacks such as spoofing or presentation. An attacker can attain illegitimate access to the system through the spoofing attack. *2D spoofing attack* is an example of such attacks which deludes the system by use of a facial equivalent of known user. Since the image or the video of the person can be obtained effortlessly, it makes the system highly vulnerable.

Face liveness detection or *face spoofing detection* is been developed against 2D spoofing attack. It is a procedure to direct if an image is real or fake [18] before the detection of the face. If an image is found faulty, it is filtered out of the recognition system. It involves two different

methods: *software – based* liveness detection and *hardware – based* liveness detection [6]. The existing methods of face liveness detection [6] are shown in Table 1 below.

Table 1: Methods against 2D spoofing attacks

Category	Sub-category	Description	Typical Algorithms
Software -based	Texture	Capture difference on visual and tactile quality between real and fake faces	local binary patterns (LBP) , Fourier analysis , color texture analysis , etc.
	Structure Information	Capture difference of structure properties between 3D real faces and 2D-planar attack	diffusion speed , facial feature trajectories , defocusing techniques , optical flow , etc.
	Liveness Sign	Capture natural human movements	Detection of eye blinking, head rotation and lip movements
	Image Quality Analysis	Analyze the quality of the real face and 2D spoof face images	Analysis of image specularity distribution , image distortion and general features
	Hybrid Methods	Combine different kinds of information to assist the detection	DMD-LBP-SVM, which combines texture and structure information
Hardware -based		Use additional hardware to measure the properties of a live face, like temperature and the reflectance of the subject	Infrared camera , 3D camera, multiple 2D cameras , light field camera, etc.

4.6.1 Flash and No Flash Image pairs to distinguish faces

This method takes advantage of both hardware based and software based method [6]. Flash is implemented to enhance the accuracy of software based methods in texture and structure information. This highlights the differences between the fake and real face. As per Patrick et al., the entire face is split up into three regions and Sparse Network of Windows (SNoW) classifier [6], a method based on Successive Mean Quantization Transform [6] is applied to it. This distinguishes the 2D spoofing attack precisely. The original face can further be differentiated from the duplicate one by machine learning algorithms such as Support Vector Machine (SVM). This simplifies the performance by using the extracted features in a two – class classification problem [6].

4.6.2 Dataset

As per the experiment performed by Patrick et al., a dataset consisting of 50 images was taken into account, which includes 42 males and 8 females with the age from 18 to 21 [6]. Each individual is made to sit in - front of a camera and two images are taken, out of which one is with flash and another one is without flash [6]. The flash lies above the camera. The distance between the participant and framework is taken into consideration so as to observe the effects of distance to background. An uneven illumination is created by placing a lamp source to create unbalanced lightening environment. 1000 samples are collected in total by taking at most 20 images of the legitimate user. Another thermal image method was considered to carry hardware based experiments. This takes environment factors into consideration.

4.7 Face recognition on Devices used by Consumers

The traditional systems used to secure the user data, are prone to numerous attacks, especially in case of consumer devices such as smart phones, laptops, desktop computers and so on. Though the systems remains vulnerable to elementary spoofing attacks, it requires sophisticated systems to overcome attacks such as *Replay Attacks.* In biometric systems such as facial recognition, the vulnerability of the system increases, where the digital biometrics is captured by malicious attackers for using it later.

4.7.1. Researched Approach

The approach to overcome these attacks is done by bypassing the replay attacks through liveness detection. This technique uses the digital watermarking of face images [7], and involves the following:

A. Frame Differencing: Since consumer devices are of wide range, these are operated in varying environment. This techniques aims to counter the differences. The difference in frames due to illumination reflecting from window causes a change in subsequent frames. These are been isolated for analysis. If Wo be the initial frame and Wη be the subsequent frame windows then isolation obtained, representing the Black response is:

$$\Delta W\eta = \min(\max(W\eta - Wo, 0), \alpha)$$
$$(\alpha=255; \Delta W\eta \in [0,\alpha]) \quad (1)$$

B. Constraints with current Consumer Devices: The current technology obtained is not sufficient in nature and contains the following factors that causes errors in face recognition [7]:

1. Face is constantly moving causing a delay in detection.
2. Screen resolution is poor
3. Camera devices have different behavior. Each of these devices have its set of drivers which can be very different from other devices.
4. Increased resolution results in decreased frame rate.
5. Contexture and replicated light levels are not easily predictable
6. Non – atomic imaging: digital cameras just scan an image.

C. Capture Algorithm: The algorithm is designed to capture the images of an object that are illuminated by screen of device. As per Daneil et al., different cameras react differently to the automatic settings including focus, brightness, saturation and white balance [7], each of its properties should be taken into account. This allows it to adjust automatically to the surroundings and improve the consistency among them. This illumination level is dependent on the Automatic White Balance (AWB). AWB corrects the white balance of

the images prior to the capture. Algorithm aims to find the brightest pixel in the image, and make it as white as possible. Thus colour responses are adjusted to make reflected colour classification difficult.

D. Algorithm for Color Classification: The sequences of color can be estimated by the Support Vector Machine (SVM) in order to determine the reflected color [7]. The three frame of colour illumination are captured through the Capture Algorithm. This follows the identification of sequence of Black frame followed by the coloured frame. This then identifies the beginning of each set of three colour frame [7]. This adds the repetitiveness to the classification process and improves the correct colour classification.

V. INFERENCE

The paper comprises of the various existing methodologies used currently in face spoofing detection. Although, being very efficient and productive every system has its own vulnerabilities. For example, Image Distortion Analysis has low robustness is highly complex [1]. Presentation Attack Detection involves immense evaluation and its performance tends to degrade with time [2]. Color Texture Analysis [3], Liveness Detection Using Flash [6] and Diffusion Speed Model [4], all three of them are vulnerable to malicious attacks due to lack of datasets value and can only be used for a particular kind of environment. Face Recognition on Consumer Devices have proven to be ineffective on some smart devices and have a limited success rate [7].

VI. CONCLUSION

The given case studies summarized the development taken place in various aspects in order to control the spoofing attacks. The countermeasures, though being useful are limited to the particular use and cannot be applied to universal usage. Thus there is a requirement to have rigorous efforts in future works in this field. It has been observed that past work lacked a standard estimation procedure that is necessary to assess the impact of these countermeasures on the current biometric systems. This adds necessity for the future work to adapt a method so as to take the countermeasures into consideration. The research direction leads to a focused work in classification strategies so as to overcome avoidable errors present in the current system. Finally, there are some open issues in this field which requires detailed research in order to upgrade the efficiency and ruggedness of the biometric systems.

VII. REFERENCES

[1] Di Wen, Hu Han, and Anil K. Jain, *Face Spoof Detection with Image Distortion Analysis*, IEEE.

[2] R. Raghavendra, Kiran B. Raja, Christoph Busch , *Presentation Attack Detection for Face Recognition using Light Field Camera*, Norwegian Biometric Laboratory, Gjøvik University College, Norway.

[3] Zinelabidine Boulkenafet, Jukka Komulainen, Abdenour Hadid , *Face Spoofing Detection Using Colour Texture Analysis*.

[4] Wonjun Kim, Sungjoo Suh, Jae-Joon Han,*Face Liveness Detection From a Single Image via Diffusion Speed Model*, IEEE

[5] Mahmood Sharif, , Sruti Bhagavatula, Lujo Bauer, Michael K. Reiter, *Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition*, Carnegie Mellon University,Pittsburgh, PA, USA and University of North Carolina,Chapel Hill, NC, USA

[6] Patrick P.K. Chan, Weiwen Liu, Danni Chan, Daneil S Yeung, Fei Zhang, Xizhao Wang, Chein-Chang Hsu, *Face Liveness Deetection Using a Flash against 2D Spoofing Attack*, IEEE

[7] Daneil F. Smiths, Arnold Wiliem Member, IEEE and Brian C. Lovell, *Face Recognition on Consumer Devices: Reflections on Replay Attacks*: Senior Member, IEEE

[8] Gustavo Botelho de Souza,, Daniel Felipe da Silva Santos, Rafael Gonçalves Pires ,Aparecido Nilceu Marana, João Paulo Papa, *Deep Texture Features for Robust Face Spoofing Detection*, IEEE

[9] Santosh Tirunagari, Norman Poh, David Windridge, Aamo Iorliam, Nik Suki, and Anthony T.S. Ho, Detection of Face Spoofing Using Visual Dynamics.

[10] Alireza Sepas-Moghaddam, Fernando Pereira, Paulo Lobato Correia, *Light Field based Face Presentation Attack Detection: Reviewing, Benchmarking and One Step Further*, IEEE

[11] Abdenour Hadid, Nicholas Evans, S´ebastien Marcel and Julian Fierrez, *Biometrics systems under spoofing attack: an evaluation methodology and lessons learned*

[12] Lei Li, Paulo Lobato Correia, Abdenour Hadid, *Face recognition under spoofing attacks: countermeasures and research directions*

[13]: Debaraj Rana, Nrusingha Prasad Rath., *Face identification using soft computing tool*, IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT).

[14] Boulkenafet, Zinelabidine, Jukka Komulainen, and Abdenour Hadid, Face Spoofing Detection Using Colour Texture *Analysis*, IEEE Transactions on Information Forensics and Security.

[15] SpringerNature, *Biometric Security and Privacy*

[16] www.ijritcc.org

[17] www.cs.cmu.edu

[18] www.archive.org

[19] Advances in Computer Vision and Pattern Recognition