Face spoof identification strategies and implementation: outcomes and insight

Bhupinder Kaur
Lovely Professional University
Phagwara, Punjab, India

Anirban Chakraborty
Lovely Professional University
Phagwara, Punjab, India

Ruchika
Lovely Professional University
Phagwara, Punjab, India

ABSTRACT: **Applications ranging from fingerprint replication to verification of mobile payment are widely used to recognize instant profile. The recognition of face recognition has raised issues about experience spoof hits (also often known as biometric sensor display attacks), where an image or maybe video of an authorized person's experience could be utilized to access services or facilities. While a selection of face spoof detection methods have been introduced, the ability of theirs to generalize wasn't sufficiently addressed. We provide an efficient and extremely powerful deal with spoof detection algorithm primarily based on an evaluation of picture distortion (IDA). In order to develop the IDA include vector, four individual capabilities (specular reflection, chromatic moment, blurriness, and deviation of color) are eliminated. To differentiate between genuine (live) and phony faces, an ensemble classifier, comprising of several SVM classifiers trained for different deal with fake strikes is utilized. The suggested remedy will likely be expanded to detecting multiframe deal with spoof in video clips with a voting based scheme. We also compile the MSU movable deal with spoofing program (MSU MFSD), a face spoofing application.**

Keywords: MFSD, MSU, MatLab, IDA,SVM , idiap, ALM-SVM, CASIA database

I. INTRODUCTION

There is a lack of clarity in terms of optimizing the techniques for integrating facial recognition into broad deployment programs for facial recognition from restricted imagery and cooperative subjects (e.g. reduction of Id card) to uncontrolled image scenarios with non-cooperative subjects (e.g. lists. This research examines the question of the identity in a number of knowledge sources (faces, videos tracking, facial sketches, 3D image and demographic details) of an individual person both in enclosure and free range modes of identity. Seeing identification of attacks demands that identified users wrongly deduce their presence by creating artificial facial replicas to bypass biometric security controls. Such attacks may be done successfully by printing or displaying remotely pictures on notebooks, smartphones and more. The identification of identity features is a commonly employed countermeasure method used to differentiate between natural and artificial characteristics. Automated face recognition has drawn growing attention in various access control systems, in particular for cellular unblocking. With face-unlocking apps in the Android mobile operating system, facial recognition has become a biometric app screening tool comparable to the iOS Touch ID. Facial recognition does not need any extra sensor, since both smartphones have camera in the front. Nonetheless, concerns about face spot attacks of facial detection systems must be handled in a similar way to other biometric modalities, especially in sensory and non-cooperative topic situations [3] and [2]. It is fairly secure to acquire biometrics, such as finger-printing, palms and exposure to imagine a person's face or facial identity (e.g. from a video camera or social media). In contrast, the expense to launch a facelift assault is very low, e.g. written script, script or video replay (Fig. 1). Commercial off-the Shelf (COTS) face identification mechanisms are not well equipped to distinguish between counterfeit faces and actual faces. Cots identification of facial recognition systems (COTS11) is evaluated in pairings with the gallery's actual faces. More than 70% of test videos (fake images) were combined with COTS 1, which indicates that COTS1 can not differentiate effectively between real and false images.

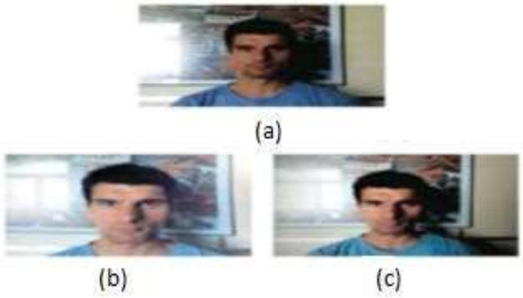


Fig: 1 Imagine a person's face or facial identity

Numerous experiments on facial spoof sensing [4] have been conducted [7]–[12] focused on the susceptibility of facial recognition to face spoof assaults. However, there are few reports available since the images (videos) used for testing and training in the same imaging conditions has been registered. Robust facial disruption algorithms (or anti- population) that can be generalized well into new imaging contexts and environments must be developed.

FACE SPOOFING:

Biometrics refers to technologies that measure and analyzes the properties of the human body. Specifically physical features, including fingernail, faces or iris patterns and movement features (e.g. accent, signature and walking styles) can be divided into 2 types, i.e. This being the case, the possibility of theft, which is referred to equally as spoofing, is one of the major problems in different biometric recognition systems. Impostors are successfully manipulating and mimicking other licensed data to gain illegal access to the biometric network, while the individual person does not agree. Examination of spoofing assault detection activities establish entirely opposite perceptions of mistreatment [9]. Throughout part of the study, the revolutionary spoofing technique for facial statistics is given for lightweight physiological property identification. Fake faces are usually classified into 2 classes: optimistic and negative. The positives have limited variation, but the negative ones include the face of the spoof in the images, dummies or recorded videos.

II. LITERATURE REVIEW AND RELATED WORK:

Li et al. wrote, as far as we understand, one of the first research on spoof identification is in 2004[13]. The growing phenomenon of facial recognition in terms of access control [4][7]-[12] has drawn considerable attention in this subject over the past five years. One of the key areas of emphasis in the EU sponsoredFP7, Tabula Rasa [14], is the reliable biometrics under spoofing attacks. Here we give a quick overview of the algorithms described in the literature, along with their strengths and weaknesses in terms of robustness and overall application, and (ii) the reaction and usefulness in real time. The strategies that have been documented that, on the basis of different signals used before spoofing, be divided into four categories: i) movement-based strategies, (ii) texture-based methods, (iii) picture coherence analysis and (iv) methods on the basis of other indicators.

(i) Motion-based approaches: these techniques are mainly developed to combat written threats, and are very relevant to the point of vitality: the involuntary gesture, such as blinking eyes [10], mouth motion [15], head rotations [11], of organs and muscles on a living neck. As motion is a quantitative function of video frames, these techniques can be extended well than the texture-based approaches described below. The shortcomings of motion-based approaches are, however, clear. The frequency of the human physiological rhythm from 0,2 to0,5 Hz is limited in the intensity of face motion[12]. Therefore, the aggregation of healthy vitality for facial spoof identification requires relative long (usually > 3 s). In comparison, gesture-based approaches may be quickly bypassed or misleaded by certain gestures, such as background action, unrelated to the motion of the face or shifting in visual attacks again.

(ii) Texture Based Methods: In order to fight depicted picture and replay video assaults, texture dependent approaches were used in mock-facial imaging to eliminate imagery artifacts. In [18], the writers indicated the differentiation of texture properties (such as LBP, DoG, or HOG) and valid faces on spotted surfaces. Idiap and CASIA repositories have been extremely popular in texture-driven approaches. The Idiap index has been decreased by the half-total error rate(HTER)5 from 13.87% in [4], and 7.60% in [16], to 6.62% in [12]. Compared to motion-based techniques, textures only need one image for spoof identification. However, some texture-based methods demonstrated a low potential for widespread use. Work in [16] reveals that HTER has dramatically improved in two texture-dependent methods (proposed in [4] and [16]) under cross-database scenarios (where training sets and experiments are focused on different face databases). Due to the nature of hierarchical structures, which are essentially data-driven, it can be over-adapted easily to a specific light and visual conditions and even to certain situations not properly converted into datasets.

(iii) Techniques focused on image content analysis: In a recent study[22], 25 photo coherence tests, including 21 complete reference and 4 non reference intervention measures, proposed a biometrical method for the detection of iris, fingerprints and facial portraits. In contrast with [22], our research is different from [1) While 25 features are required for successful results [22], there has been no face-specific details on the design of insightful apps for facial spoof sensing. At the opposite, four characteristics are precisely configured to reflect face in our program and we illustrate the utility of spoof face recognition. (2) We use both the Idiap and CASIA databases, the two basic repositories of the public domain, while [22] the authors extended their method only to Idiap Replay database. (2) (3) In addition intra-dominium scenarios (although equally defined, while cross-validation is required) have been used to train and test modality, although work in [22] is planned to establish a basic instrument of detection of liveliness in different biometric modalities. The suggested approach, by contrast, seeks to boost the likelihood that the biometric community actually addresses for generalization under cross-database conditions.

(iv) Certain Cues Methods: In the face-spoof counter-measurements markers derived from other sources than 2D images, such as 3D depths[19], IRs[6], spoofings[20] and voice [21], are commonly applied. The consumer or facial recognition system, however, has specific requirements and is only a small range of applications. Examples of this involve an IR sensor[6], a microphone and voice analyser[21] and a large number of facial images[19] which were needed. In fact, the spoofing mechanism in the background approach suggested in [20] may be circumvented by disguising it. Table I deals with the four types of Spoof ID. Both four strategies are combined to also be used to recognize facial spoof with different markers. The authors found, for example, in [12] that the correctly magnified motion cue [23] enhances texture-dependent approach efficiency (HTER= 6.62% of the movement magnification of ibia database, compared to HTER= 11.75% of all characteristic LBP data). Through combining the Histogram of Oriented Optical Flow (HOOF) with the movement rise, the writers have shown the maximum performance on the Idiap website. Yet motion enlargement, restricted to a human physiological model, does not attain the reported significance (13) without a sufficient number of video frames (> 200 frames) being obtained. While a few facial spoof identification methods have been published, none of them may well generalize cross-database scenarios[17]. No study of how facial spoof detection methods are carried out is possible, especially in cross-database circumstances. The intranet equipment (for example, picture & image on the monitor), the computer, environmental variables and even the subject matter are believed to be decided by a facial enmity sensing system in an intra-domain case. The key differences in the intranet and cross-site scenarios are as follows: This rule does not extend in most individual circumstances. The success of the facelift program data base is just the maximum degree of productivity that cannot be found in actual applications.

(i) Variations in mock newspapers, images, atmosphere and themes may be rendered in a cross-database situation during the device production process and throughout the network implementation process. Such cross-database success thus further illustrates the actual performance of a device found in real applications.

(ii) Proven techniques, in specific texture characteristic methodologies, widely utilized technologies (e.g. LBP) capable of collecting and distinguishing facial information on a single topic (to identify the face). Therefore, where the same attributes are used to differentiate a single face from a different position, then redundant or more individual detail is used. All variables restrict the capacities of existing methods to generalization. We suggested to deal with this question with a variety of applications that rely on image distortion analyzes (IDA), with an actual answer. The suggested method would not attempt to gather knowledge on existing strategies from faces but will try, by utilizing the different reflective properties of such materials as face tissue, paper and glass, to identify variations in the contents of facial photographs. The findings of the tests indicate that the approach introduced is more universal.

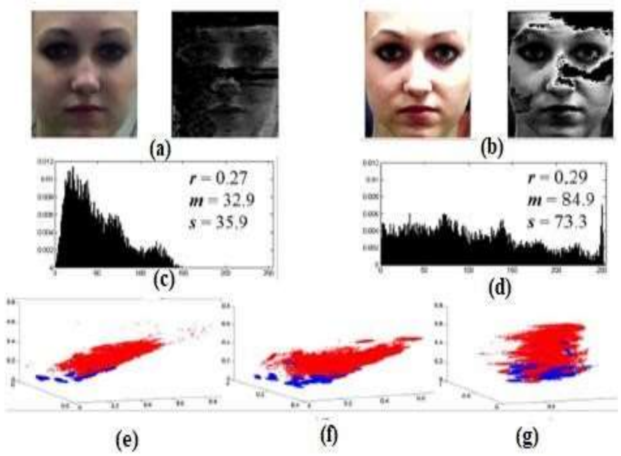


Fig 2. Specular Reflation Features

***1) Face Distortion Analysis-derived features Classifier experts are merged in order to offer the final binary decision: real or facial fake*.**

A.) Specular Reflation Features The facial reflex was widely used to prevent strange reflection[26] and to normalize facial illumination[25]. In this article, the specular reflection portion is a single-source, (ii) a single-source, (ii) a standard, and (iii) not over-saturated, input or video frame using the iterative (including 6 iterations) approach suggested under [26]. Because indoor images are taken mostly in the sense of fairly controlled lighting (Idiap, CASIA and MSU databases), these three assumptions are reasonable. The disparity between the specular reflecting components of the real face and their respective parody, as seen in Figures 2 (a, b). Once we have calculated the reflective picture Is variable, we define the three-dimensional distribution of intensity specularity: I specular pixel percentage r, ii) speculation pixel intensity µ, and iii) speculation pixel intensity µ (variance). Nevertheless, the method in [26] relies on a chromatic difference analysis, as stated in[25], which extracts specular components that often misclassify the Mono-Chromatic Regions as specular components. To fix such defects, we remove high-resolution monochromatic pixels from Specular Components (as in [25]). Relevant specular pixels are present mainly in the spectrum of intensity (1.5µ, 4µ). The three-dimensional hypothetical reflex properties determined in the MSU database display the true face and spoof of the topic. Figure 2(a-d) Figure 2 (e-g) reveals, in Idiap planning, Idiap analysis and MSU science, the 3D distribution of the specular reflection characteristics of true and false facets. Such distributions imply that a classifier trained on the Idiap training set will work well on both the Idiap and MSU test sets with a different reflection function.

Illustration.2. The specular reflection characteristics example. (a) a true image of the face and the detected reflecting element of the specular; (b) a spoof face (video replayed) and a detected reflection component of the specular reflection; (c-) histograms and particular feature values in (a) and (b) respective of the specular reflecting components; and(e-) distributions of the specular reflection components in the idiap formation, ibid.

B.)Blurriness Highlights Spoof images are frequently discarded in cell phone cameras for short distance spoof assaults. The explanation is that there is typically small size of the spoofing medium (print paper, laptop screen and cell phones), so the attackers will place the media close the monitor such that the limits of the target medium will be blurred. It helps to defocus spoof faces and the blurred picture attributable to defocus may be seen as another sign for anti-spoofing. Two forms of bubbly properties (referred to as b1 and b2) have been suggested respectively in [23] and [24]. In [23], the difference between the original image and its blurred version is measured. The through the disparity, the less the complexity of the initial image. Blurriness in [24] is calculated on the basis of the average border width in the pixel. Both these two approaches yield a blurrency score of 01 (without a clearly identifiable picture as a reference) but emphasize specific measures of bubble.

C.)Facial photographs recaptured tend to show a different color spectrum relative to colors of real facial pictures. Chromatics Moment apps This is because printing and display devices have an incomplete color reproduction feature. In [25] for the detection of retrieved images, this chromatic damage has been investigated, but its efficiency in face detection is unknown. Since the absolute distribution of color depends on the light and the variations of the camera, we propose invariant characteristics to detect abnormal color in spoof faces. That is, we convert first to HSV (Hue, Saturation, and Value) the normalized facial image from the RGB space, then measure the mean, variance and skew of each channel. Because these three characteristics are identical to each canal's three mathematical moment, they are often regarded as chromatic momentary characteristics. In addition to all three characteristics, two additional characteristics are the pixel percentages in the minimum and maximum histogram bins for each display. The chromatic moment function dimensionality is then 5 to 3= 15.

D.) The difference between authentic and spoof faces is the diversity of colors. Authentic images, in fact, appear to be wealthier. The color reproduction loss during image / video retrieval tends to dissolve in the spoof faces. We follow the method used in this paper [25] to measure the diversity of the image color. First of all, color quantization is carried out on the standardized face image (32 steps in the Red, Green and Blue channels). Two color-distribution measurements are then pooled: I the histogram bin counts of the top 100 colors that occur most frequently, and (ii) the amount of specific colors that occur in the normalized face picture. The color identity function has a dimensionality of 101. The four feature forms (specular reflection, flutter, chromatic moment, and variety of colors) mentioned above are eventually merged, generating a 121-dimensional IDA function vector. While the IDA vector is extracted from the facial region, it only contains information concerning the distortion of the image and not any facial appearance characterization. Consequently we expect that the IDA feature can alleviate the problem of bias in the usual texture characteristics.

2) Process A in Classification:

A.) Given that we want the effective face spoof detection method with a strong generalization and fast response, an effective classifier for the IDA characteristics extracted is desirable. We have agreed to use the SVM [18] in Lib SVM library [20], after SVM [26] has worked in signal processing [17], pattern detection and classification applications [18],[19]. There are some SVM alternatives for the treatment of large-scale classification issues, such as LIBLINEAR[11] and ALM-SVM[12]; but, in terms of still photographs, video tracks and topics, most of the public-domain face spoof data bases (including databases included in our experimental work) are restricted in complexity. Each group of training data is trained for an SVM classifier with RBF kernel, with cross-validation parameters optimized. At the other side, various spoof assault conditions in the IDA function space are known. Although samples of attacks written appear to be less in comparison than real tests, for example, tests for re-plays attacks are more in comparison. Different types of attacks can often have different features of chromatic distortion. Thus an ensemble classifier is best adapted to counter multiple spoof attacks instead of practicing a single binary classifier. We create different groups of training samples for a specific Spoof database as follows: First, the Spoof samples are separated into K classes based on the form of attack. Second, a particular training scheme is designed by taking into being K training sets and mixing all actual samples with one collection of spoof samples. In our experiments the Ensemble classifier performs better than training a single classifier on the entire sample by training two constituent classificatory in two different spoof target classes, that is, a written target and a replay assault (K= 2).

B.) Multi-Frame Fusion The multi-frame fusion device is built to produce a more consistent facial spoof identification output in the video because of the face spoof classification usable for one single image. The consequence of classification is paired with a voting method to achieve the video spoof identification ranking. If more than 50% of their videos are counted as genuine face photos, a face video is considered to be genuine. Given the usage of N photos, a multi-frame fusion extension helps one to equate the proposed method's output with state-of -the-art videos provided the same duration of study.

3. Databases Face Fake

A.) A significant number of recent articles have developed and evaluated their algorithms in proprietary Spoof repositories to determine the efficacy of spoof detection algorithms [6], [10], [11], [19]. Although only a limited number of scholars have released their fake data bases [4],[7]–[9],[24],[25]. This segment provides a brief overview of the Nuaa Image Imposter database[8], REPLAYATTACK Idiap database[4] and CASIA image anti-spoofing database [9], three databases with the public-domain profile-photo-spoof. A few other repositories for facial spoof sensing are accessible in public domains. Throughout the area of visual spoof-detection, the VidTIMIT Audio-Video database (43 subjects)[24] and the DaFEx database (8 subjects) [25] are both included, but they are less desirable for experimental tests due to small scale and spoofing. One of the first public fake repositories was the NUAA Image Imposter database [8] launched in 2010. There are 12 614 pictures of real and assault attempts by 15 subjects (extracted from 143 videos). Furthermore, the NUAA site contains only hand-held typed picture assaults. In the same circumstances (controlled lighting and adverse) of creation, face spoof attacks were generated by forging live testing trials of the same subjects utilizing typed images, pictures / videos seen on the handheld telephonic device, an Idiap REPLAY Assault database[4]. In 2012, it contains 1.300 real video recordings as well as assault attempts of 50 specific subjects. The 2012 CASIA Face Anti-Spoofing Database [8] comprises of 600 authentic video images with 50 separate personalities, as well as assault attempts. Although the CASIA collection is significantly smaller than the Idiap collection, it includes more varied data collections (high-resolution NEX-5 image, low-grade USB cameras) and variations in the face (variations of speech and pose) and attack attempts (warp video, screen cut and HD display).

In terms of sample size, purchasing tool, assault form and sex, class and race proportions of items. A major drawback to all three counterfeit databases is that web cameras or good end video cameras have caught all datasets. There are no public domain counterfeit sites that are filmed by cell telephone cameras. Face spoof recognition is tested by the cell phone close-up cameras: i) They typically include lower quality, a limited dynamic range and correct measuring and auto focus capacities. As a result of defocus, under, or over exposure, videos and photographs captured by such cameras usually have poor quality. As these degradations in the picture content exist both in actual photographs and in fake images, the variations in face-detail and facial distortion between true and counterfeit visual images can be minimized. ii) It is not merely to render the identification phase more complicated but to recreate a practical situation in the cell phone face spoof database. The gap used to initiate spoof attacks is another obvious property of such repositories. The intruder in the Idiap database inserted the spoof medium in near proximity to the camera (short distance spoof attack), which culminated in the spoof video becoming very wide face region. With a longer standoff [46] in the CASIA database, the spoof attacks have been developed, resulting in a smaller facial zone and less contrast in the spoof attacks.

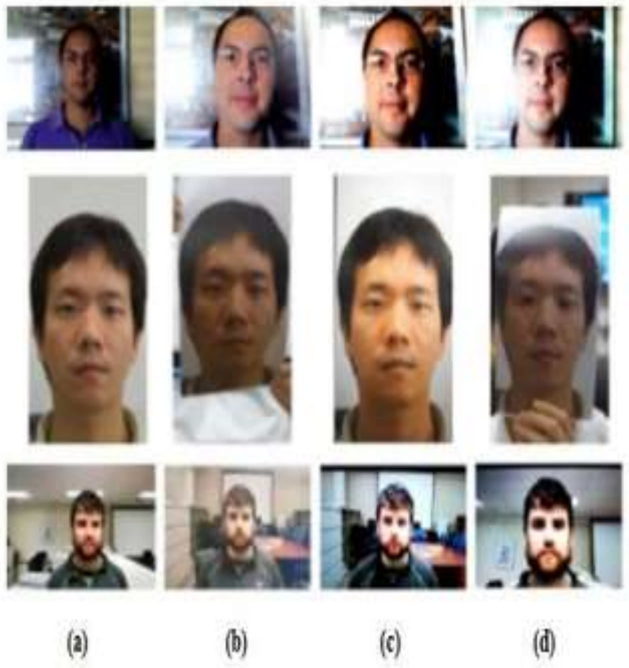


Fig. 3 shows short-range attacks for spoofing and provides MSU Mobile Face Spoofing Server (MSU MFSD) to allow cell phone device spoofing work.

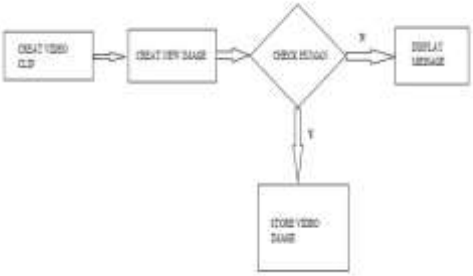
B.)The MSU MFSD database consists of 440 video clips of 55 subjects in photo and video attack attempts. In the collection of this database two cameras were used: 1) Built in laptop camera 2) Mobile front-facing camera. They are also state-of -the-art products.

1) Authentic face: The (true) subject shows the camera face, and a true face video is recorded with both Android and laptop cameras. The maximum size from the eye to the mask is 50 cm.

2) Photo Replay Spoof Attack: The Face Target Picture lies on a monitor. The device is often used to record HD (1920 videos 1088) and to create a HD video replay assault on your computer. The mobile device will be used to capture another video on mobile screen (1920 video1080) that will be replayed for mobile video playback. The HDVideo playback assault stands average 20 cm. For mobile video repeater attack, the average stoppage is 10 cm.

Fourth, PROBLEMANALYSIS Our research utilizes the whole media database as the probe to produce a single candidate's list for the person of concern, conventional facial matching approaches use specific media as the reference. In applications spanning from identification deductions to mobile payment authentications, automatic facial detection is now commonly used. This prevalence has created concern regarding facial spoof attacks (also known as biometric display attacks) in which a picture or video of a person's registered face may be used for the exposure of installations or facilities. While a variety of strategies were suggested for spoof identification, their capacity to generalize was not properly discussed.

3.) Suggested Program:-The proposed solution in this analysis increases the possibility to accurately classify the individual involved by choosing video frames using various schemes. In this work the effective and very reliable facial spoof detection algorithm is based on IDA analysis. The IDA function matrix consists of four distinct attributes (specific mirror, dull, chromatic moment, and richness of color). In this job, you can also collect MSU Mobile Face Spoof Database (MSU MFSD), which includes spoof attacks for the video I playback. e. Net. Net. The findings illustrate the complexity in distinguishing the real faces from the fake, especially in cross-databases. The approach suggested is able to reliably work at different biometric (multi biometric) characteristics. The strategies suggested provide a strong degree of defense against increasing forms of aggressions (multi attacks). Error levels are very small compared to other anti-spot attacks; the proposed approach is quick, user-friendly and powerful because of the multi-biometrics and multi-attack characteristics.



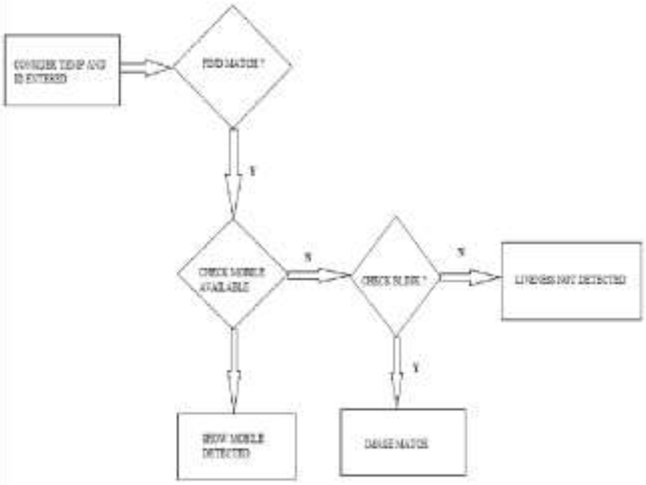


Fig 4. Flow Diagram of Suggested Program

4.) MSU Mobiles Face Spoofing Site: MSU MFSD, with the spoof attacks for video played I, in this article. Findings AND Debate. e. Web. This research proposes to conduct face defect analysis based on picture distortion analysis (IDA) unlike other existing approaches utilizing motion and structure dependent characteristics. To form the IDA feature vector are extracted four different characteristics (specular reflection, blurrence, chromatic time and color diversity). The project that proposed Matlab to act as an alternative to the front and back ends improves the possibility of properly defining the individual involved, by integrating consistency controls for fusion and video structure collection utilizing various fusion schemes.

III. CONCLUSION

In this report, it was established that the face spoof detection technology was implemented in order to enhance the reliability of the bio-metric Anti-spoofing device. It is very necessary for a program to detect and avoid attackers, in particular with a broad variety of threats, correctly. Throughout this study, an image distortion analysis (IDA)-based face spoof identification approach is suggested.

IV. REFERENCES

[1]. A. Rattani, N. Poh, and A. Ross, “Analysis of user-specific score characteristics for spoof biometric attacks,” in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jun. 2012, pp. 124–129.

[2]. Z. Wu, N. Evans, T. Kinnunen, J. Yamagishi, F. Alegre, and H. Li, "Spoofing and countermeasures for speaker verification: A survey," Speech Commun., vol. 66, pp. 130– 153, Feb. 2015.

[3]. L. Best-Rowden, H. Han, C. Otto, B. F. Klare, and A. K. Jain, "Unconstrained face recognition: Identifying a person of interest from a media collection," IEEE Trans. Inf. Forensics Security, vol. 9, no. 12, pp. 2144–2157, Dec. 2014.

[4]. I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in Proc. IEEE BIOSIG, Sep. 2012, pp. 1–7.

[5]. N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect," in Proc. IEEE BTAS, Sep./Oct. 2013, pp. 1–6.

[6]. Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," in Proc. FG, Mar. 2011, pp. 436–441.

[7]. A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IJCB, Oct. 2011, pp. 1–7.

[8]. X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in Proc. ECCV, Sep. 2010, pp. 504– 517.

[9]. Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in Proc. ICB, Mar./Apr. 2012, pp. 26–31.

[10]. L. Sun, G. Pan, Z. Wu, and S. Lao, "Blinking-based live face detection using conditional random fields," in Proc. AIB, 2007, pp. 252–260.

[11]. W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in Proc. IASP, Apr. 2009, pp. 233–236.

[12]. S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally efficient face spoofing detection with motion magnification," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jun. 2013, pp. 105–110.

[13]. J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra," Proc. SPIE, vol. 5404, pp. 296–303, Aug. 2004.

[14]. The TABULA RASA Project. [Online]. Available: http:// www.tabularasa -euproject.org/, acccessed Sep. 2014.

[15]. K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-time face detection and motion analysis with application in „liveness" assessment," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 548–558, Sep. 2007.

[16]. T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "LBP–TOP based countermeasure against face spoofing attacks," in Proc. ACCV Workshops, 2012, pp. 121– 132.

[17] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario?" in Proc. ICB, Jun. 2013, pp. 1–8.

[18]. J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in Proc. IJCB, Jun. 2013, pp. 1–6.

[19]. T. Wang, J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection using 3D structure recovered from a single camera," in Proc. ICB, Jun. 2013, pp. 1–6.

[20]. J. Komulainen, A. Hadid, and M. Pietikäinen, "Context based face antispoofing," in Proc. BTAS, Sep./Oct. 2013, pp.1–8.

[21]. G. Chetty, "Biometric liveness checking using multimodal fuzzy fusion," in Proc. IEEE FUZZ, Jul. 2010, pp.1–8.

[22]. J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," IEEE Trans. Image Process., vol. 23, no. 2, pp. 710–724, Feb. 2014.

[23]. H.-Y. Wu, M. Rubinstein, E. Shih, J. Guttag, F. Durand, and W. Freeman, "Eulerian video magnification for revealing subtle changes in the world," ACM Trans. Graph., vol. 31, no. 4, Jul. 2012, Art. ID 65.

[24]. S. A. Shafer, "Using color to separate reflection components," Color Res. Appl., vol. 10, no. 4, pp. 210–218, 1985.

[25]. O. Bimber and D. Iwai, "Superimposing dynamic range," in Proc. ACM SIGGRAPH Asia, 2008, pp. 1–8, no. 150.

[26]. PittPatt Software Developer Kit.Pittsburgh Pattern Recognition PittPatt.[Online]. Available: http://www.pittpatt. com/, accessed Jan. 2011.