International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

A Face Spoof Detection using Feature Extraction and SVM

Lovely Pal[1], Renuka Singh[2]

[1]Department of Computer Science and Engineering, ABSS Institute of Technology, Meerut UP, India
lovelypal182[at]gmail.com

[2]Department of Computer Science and Engineering, Meerut UP, India, ABSS Institute of Technology

Abstract: ***Face spoofing detection is one of the well-studied problems in computer vision. Face recognition has become a widely adopted technique in biometric authentication systems. In face recognition based authentication techniques, the system first recognized the person to verify the legitimacy of the user before granting access to the system resources. The system must be able to determine the liveness of the person in front of the camera, for example, by recognizing the face and denying the types of face presentation attacks related to photographs, videos and the 3D mask of the targeted person. Attackers try to directly or indirectly, masquerade the biometric system as another person by forging biometric traits and get unauthorized access. This work studies computer vision-based feature extraction techniques for real and spoof face imaging and combines different features in the area of face anti-spoofing.***

Keywords: Biometrics; Face Spoofing; Face Spoofing detection.

1. Introduction

The most basic security requirement is the protection of information. Traditional identification measures, such as usernames and passwords, are readily compromised. Biometric apps are becoming more popular, and they're more secure than that of other legitimate application programs. Biometrics certifies an individual's identification. In a biometric verification system, two distinct processes are carried out: enrollment as well as verification. Enrollment is the process of producing a biometric reference template for such a single individual and storing it for future comparison. Verification is the act of comparing the inquiry biometric to the references one in order to make a judgement.

Biometric features include the face, fingerprints, and palm. The most frequent face seems to be the typical biometric applications because it is simple to use, straightforward, and non-intrusive. Face recognition technologies have a wide range of applications, including surveillance videos and e-passports. The most prevalent biometric is the face. Face recognition algorithm, on the other hand, are vulnerable to assaults by displaying fake faces.

Face spoofing is a sort of attack that involves putting on a phone face in front of a cameras. Spoofing assaults come in a variety of forms, including print operations, video attacks, and 3D mask attacks. For detecting face spoofing, a secured system is necessary. The goal of face spoofing identification is to determine if a face image is real or faked. There are several techniques for faking one's face.

A spoofing attack happens when someone attempts to impersonate another individual by misrepresenting data and obtaining unauthorized access and benefits. For example, a facial recognition system may be fooled by putting an image, video, mask, or 3D model of such a targeted individual in front of cameras. Although make-up as well as plastic surgery may also be used to spoof, pictures are arguably the most prevalent source of spoofing assaults since they are easily downloaded and captured.

Facial spoofing has occurred on multiple occasions. For instance, the attacker may utilize the authorized face function on the smart device to expose a user's silent picture, or he or she might employ a printed version and view the picture on cameras. A print-based assault is another option. The researchers uncovered a malicious activity that was used to hide data fabrication and, as a consequence, unauthorized access from an user. The higher the quality of the offender, the simpler and more likely the attacker will be to get access; the greater the quality of the assailant, the greater the authorized video will display from a computing device that faces the camera. Using 3D photorealist masks with facial features of a recognized user is yet another means of disrupting. In the lack of a powerful anti-spoofing mechanism, it was established that such authentication process is particularly weak. It is becoming increasingly vital to design a good anti-spot system.

Authentication session in which the user stays in front of webcams for a brief period of time before receiving an acceptance or rejection answer from the system based on the program's detection accuracy. Furthermore, because to the fast increase and replay of smart device high definition, such passive briefings have become much more vulnerable to a variety of assaults.

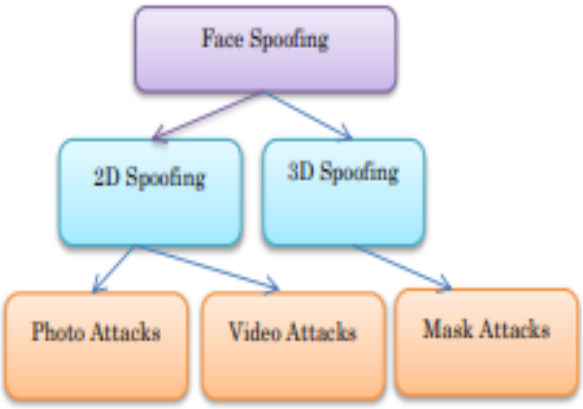
The very same mobile face expression decoding functionality proved particularly responsive to assaults in multiple other scenarios. Some believe it is overly vulnerable to simple Android publishing component. Simple trials have previously been conducted where a user may send a still image to the mobile from another machine and instantly activate the cellphone.

Face Unlock has an extremely high acceptance rate, which gives non-authorized individuals access to additional personal details, but a greater failure percentage, which is the result of various unconstrained inequalities, which also

hinders authenticated people, particularly under varied lighting conditions.

When social networking as well as internet sites begin to appear, facial features become readily available to anyone on the net and may be utilized without authorization to create fictitious allegiances. Face motion is employed to recognise the offered face conciseness in order to fight against such dangers.
Video assaults, on the other extreme, may undermine traditional biometric detection procedures. To effectively and successfully counter an attack on uniqueness from any and all sources, a dimension, complexity, be added. Aside from possible hazards, face movement offers various benefits. As a consequence, in addition to typical spoofing protections, developing a strong and efficient solution for multiple attack patterns, including human interactions, is becoming increasingly important.

Classification of Spoofing
Many studies have been conducted in the subject of spoofing detection systems in recent years. This section provides an overview of some of the approaches employed in this subject. Spoofing biometric authentication has been extensively encouraged in the previous ten years by a large number of research publications, conferences, and publications with creative concepts. Li et al. (2004) published one of the early research on face spoof recognition to our awareness. With the rising popularity of employing facial recognition for authentication mechanism, academics have paid close attention to this problem during the last five years. The diagram depicts the general classification for spoofing, which may be separated into two classifications: 2D image spoofing as well as 3D image spoofing.



General Classification of Spoofing

Photo Attacks:
This form of illegal access attempt involves presenting a recognition software with an image of a legitimate user. Hackers steal images from social media platforms or digital cameras. The attacks might be on printed graphics on paper or images projected on a screen, such as a smartphone or tablet. Photographic masks are an advanced sort of attack in photography. These are the masks with high resolution photographs. During attacks, an impersonator is put behind the attacker so that specific facial expressions, such as eye blink, may be replicated.

Video Attacks:
Such attacks are known as replayed attacks. They are the most refined versions of these picture spoofs. In just this assault, video of the user from a smart device is used instead of still photos. In this assault, video of client from a mobile camera is used instead of still photos. Some movies from mobile phones and computers are assaulted, making them more difficult to recognise not just because of their texture, in addition to their dynamics.

Mask Attacks:
In this assault, the spoofing artifacts seems to be the client's face or a 3D masks of the user's face. It is quite difficult to develop a counteraction to these mask attack. The facial 3D structure is concealed, and also the face is replicated here. Depth cues can be utilized to counter picture and video assaults, but mask attack signals are enough. Even though the prospect of bypassing a biometric system by using a mask that imitates the face of another user has been discussed for certain time.

Problem Statement:
Face recognition systems are substantially more likely to spoof or impersonate threats than that of other methods. Only with the rise of blogs on social media sites and increased camera capability has it become possible to view target individual face images or pictures. These movies and images may be immediately fraudulently seen by exhibiting them to some other user face-to-face using the face detection and recognition camera by presenting the processes on either paper sheets or digital displays.

The goal of this research is to provide more reliable, good reaction rates in surveillance film as a first step in order to build solutions enabling functionality disposal face spoof identification.

When you observe a user's face on video, check their identification by eliminating a global patterns and comparing it with the solid models in databases. Here is the official formulation of the problem: In principle, we anticipate strong user identities having dynamic face components that are actually immune to harmful behaviours will be permitted to discriminate. The solution is based on studies performed on a variety of specific matter data sets.

Aim and objective:
The traditional two-dimensional ant spoofing processes are based on three basic identification verification requirements: motion detection, form attributes, and life cycle recognition. Whenever video-playing attacks are not employed, mobilisation, while an essential picture signal, is rendered useless. Furthermore, each of these criteria has proven great or appropriate in their own particular application between assaults and authentication attempts.

To that end, this concept may be included into linked devices for essential systems like financial sector and secret data storage. The fundamental goal of this study is to build a collaborative system that incorporates texture analysis with limited interest and participation so that only authorised individuals may access it. Priority should have been given to the creation of a dependable spoof-checking system which

has been illustrated to work collaboratively well apart from different environmental distinctions like illumination or camera resolution, so that prioritizes efficiency over stability, while the majority of proposed models are recognized as completely inadequate and structurally monitored in just about all real life scenarios.

The key goals of the current research project are as follows.

1) Face - recognition software can be safeguarded against spoofing assaults by establishing spoof detection algorithms.
2) To design and implement an algorithm utilizing a software working prototype.
3) To test the efficiency of the generated model against a face spoofing detecting dataset.

2. Literature Review

Like numerous other biometric procedures, a person's identification is dependent on physiological along with behavioural features rather than information like passwords or identification card. Face recognition is a key technology used in biometric technologies. Few academics have worked over the previous several decades to enhance face recognition, but considerably less attention has been paid to another essential element, which considers the security weaknesses of spoofing.

Without anti-spoofing safeguards, most modern face biometric systems are exposed to assaults since they strive to optimise identity discrimination rather than assessing whether the displayed attribute originated from a genuine live client. A simple snapshot of the registered person's face, whether printed or put on a computer, will deceive the system. Brief surveys of prior spoofing attack efforts can be obtained. A common anti-spoofing method is liveness detection, which detects physiological indicators of life like eye blinking, face expression variations, lip movements, and so on. Pan et al. (2006), for example, suggested an anti-spoofing strategy based on the fact that humans blinking once every 2-4 seconds. It models and detects eye-blinking using the Conditional Random Field architecture. Motion analysis seems to be another often employed countermeasure since it is thought that the movements of planar things, such as video screens and images, varies significantly from that of genuine human faces, which seem to be complex three dimensional objects. Koll eider et al. introduced an optical-flow-based approach for capturing and tracking the subtle motions of various facial components, assuming significant facial parts move differently in actual faces than in pictures. Bao et al.(2016) exploited optical flow for motion estimation in another paper to identify assaults created using planar media like prints or displays.

Studies on a personal database revealed a 6% false-alarm rate vs a 1 % false-acceptance rate. Another type of anti-spoofing technology is based on the examination of skin features like skin texture and reflectance. Li et al., (2010) for example, presented a technique for identifying print-attack face spoofing. The approach is based on examination of 2D Fourier spectra, with the assumption that photos are often smaller in size and include less high-frequency elements than actual faces. This method may work well enough for downsampled photographs but is unlikely to perform well for higher-quality images. However, the database utilized in the trials is not publically accessible.

Multi-modal analytics and multi-spectral approaches are two further anti-face spoofing strategies. Face recognition combined with additional biometric traits like gait or speech is inherently more difficult to fake than uni-modal techniques. Multi-spectral pictures may also be used to analyze the reflectance of object surfaces and so distinguish between real and fake faces.

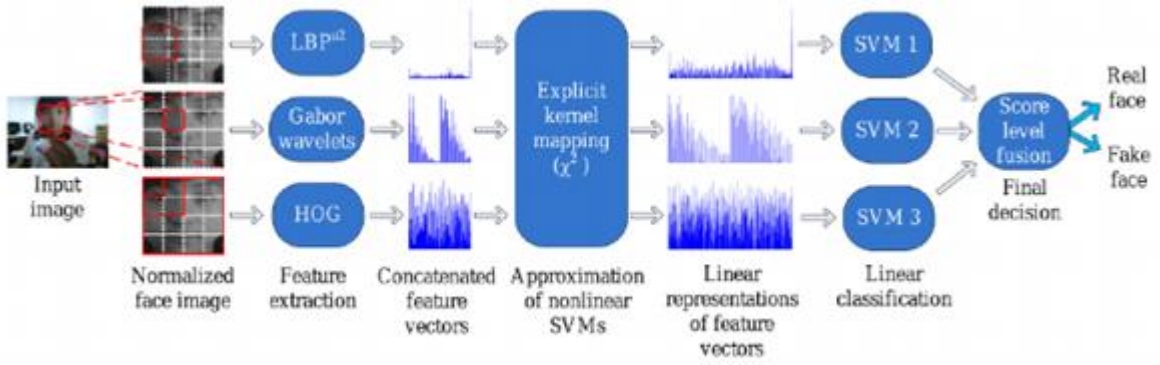
To identify spoofing assaults, Bai et al. (2004) employed micro-textures taken from secularity element of a recovered picture using a linear SVM classifier. The main disadvantage of this technology is that it demands high resolution input photographs to distinguish the fine micro-texture of the utilized spoofing medium. Another intriguing technique was presented by Gao et al., (2013) who employed a collection of physical properties to distinguish between recorded and actual photos.

Most contemporary approaches for spoofing detection tend to be either exceedingly complicated (and hence impractical for real-world face biometric systems needing quick processing) or employ non-traditional imaging systems (for example multi spectrum imaging) and gadgets . As a result, we offer a method based upon highly discriminating textural and local form characteristics, which uses standard webcam-quality photos and does not require user interaction.

Spoofing Detection using Texture and Local Shape Analysis

Face pictures obtained from printed photographs may appear visually comparable to those captured with live faces. As a result, in the originally entered space, all of these pictures would be considerably overlapping Zhenqi et.al(2015). As a result, an appropriate feature area is required to separate the two groups. The major difficulty is determining how to generate such a feature space. Our strategy seeks to understand the subtle distinctions between photos of genuine faces and those taken from face printing, and then develop a feature space that highlights those variations.

A detailed examination of the contrasts between genuine faces with face prints indicates that human features and prints reflects light in distinct ways, owing to the fact that a person's face is a sophisticated non-rigid 3D entity, even though a photograph is just a planar rigid object. Some surface qualities of genuine faces and prints, such as pigments, vary as well. These two unique qualities might result in various specular reflections and colors. Furthermore, face prints frequently contain print artifacts like jitter and banding, which may be discovered using texture and localized shape analysis on homogeneous or smooth regions. Moreover, spoof assaults using face prints tends to produce some overall picture blur as a result of, for example, a poor resolution printing equipment or fast motion generated through simulated photo-attacks. Examples of possible indicators for detecting face printing spoof.



Block diagram of the proposed approach

According to Kumar et.al (2019), Anti-spoofing strategies for the face have garnered a lot of attention, and numerous anti-spoofing strategies have been proposed in retrospective research. Modern image-based techniques focus on picture qualities and functionality, therefore they use hand-crafted features like LBP, SIFT, HOG, and SURF, together with shallow classifiers, to distinguish between real and artificial faces. Because these hand-crafted characteristics are constrained to certain spoofing patterns, scene circumstances, and spoofing instruments, their universality is limited. Deep approaches based on Convolutional Neural Networks (CNNs) have recently emerged as an alternate method for enhancing the efficiency of anti-spoofing strategies by learning a discriminatory representation from start to finish.

Whereas the data-driven functionality learning improves spoofing detection accuracy, such methods fail to capitalize on the essence of spoofing patterns, which include skin details, colour distortion, moire trends, glass ability to reflect, shape deflections, and so on, because they develop models for such current dataset as well as fail to generalize in cross-dataset configurations. They are especially sensitive to lighting as well as lighting distortion because they are constructed on controlled and biased datasets. As a consequence, over fitting as well as poor generalization to novel patterns and contexts hamper these systems.

3. Methodology

In this study, the problem of the study may be seen as a classification with 2 categories. First class seems to be the actual pictured real photo class, and the second category is the actual depicted real image category. To identify photo spoofing, the suggested approach employs several opposing properties and textures of acquired and recaptured pictures. Every function is retrieved, and the attributes are stored in a database. The picture is then processed such that it has the same properties as the test set and can be categorized as original or faked using supported vector machine.

Input Image

The input image is drawn from a collection of face spoof detecting images. CASIA FASD now comprises a database which covers a wide range of probable assault permutations. This database contains 50 actual subjects, and the false faces are high-quality recordings of real faces. Considering three image attributes: low quality, high quality, or quality. Three counterfeit assaults are carried out, comprising warp pictures, cut-offs, as well as video attacks.

Tools and Techniques

MATLAB, an abbreviation for Matrix Laboratory, seems to be a high-performance software tool for numerical calculations. It combines mathematical computations, visual analytics, including coding in such a user-friendly environment where both issues and solutions are shown in intimately familiar cognitive science.

MATLAB Simulator

The goal of MATLAB was always to make it simpler to utilize matrix technology developed by the LINPACK as well as EISPACK programs. Simulation tool now includes the LAPACK and BLAS modules, which attempt to merge cutting-edge innovative tech into programming for matrix mathematical functions.

MATLAB seems to be an interactive system that includes an array and its fundamental data component but does not need geometry. This effectively enables users to interact with the computer, particularly those using matrix and vector formulae, in a fraction of the time required to construct a program in a parameter-free computer language the same as C. MATLAB is the industry benchmark for high-end analysis, development, and evaluation. MATLAB also have been able to advance above a white period with the cooperation of a large number of users. At institutions of higher learning, it is the favored way of teaching and specific classes in mathematics, engineering, and research.

MATLAB Application Program Interface:

It is a framework for developing C and FORTRAN programs that interact with the MATLAB. It includes the ability to call MATLAB processes (developed control), use MATLAB as such an algorithmic processor, also read and write MAT-files.

Image Processing Toolbox:

Image Processing Tool Box is a collection of learning algorithms and simulation modeling for machine learning, evaluation, visual analytics, and numerical modeling. Several of the elements that are extremely possible include picture enhancement, image deblurring, feature identification, noise removal, segmentation techniques, spatial modifications, and image restoration. There are several multithreaded tools functions to take use of multi - core processors as well as multiprocessor machines.

Picture Processing Toolbox supports a variety of file format, featuring spectral resolution, megapixels camera magnification, ICC-compliant colors, and the stereoscopic images. You may explore a neighborhood of pixels, alter

comparison, generate shapes or scatter plot, and try to impact regions of interest using graph applications. Individuals may use toolbox techniques to restore degraded photographs, diagnose and also measure characteristics, evaluate contours and patterns, and change color balance.

4. Results and Discussions

The suggested approach has been implemented in real time utilizing software approaches. In MATLAB, a personal image database was constructed. MATLAB includes a plethora of built-in functions linked to numerous fields that allow for the simple execution of complicated mathematical processes. A variety of MATLAB functions relating to Image Analysis Toolbox, graphics, fundamental mathematics, and so on were employed in this study project. The built-in editor windows in MATLAB was used to construct scripts for different phases in the programming process.

Algorithm Steps:

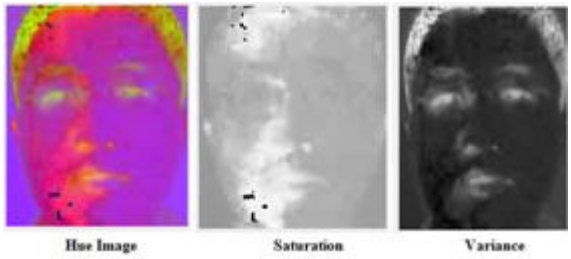
- As illustrated the initial stage is to enter genuine picture frames for each individual. The viola jones method is then applied to the input picture to recognise and reduce the face region.
- To produce homogeneous pixels, the chopped facial region is resized to 320x240 pixel size throughout the preparatory processes.
- The cropped picture is then transformed from RGB true colour style to Hue Saturation as well as Variance format, and also the characteristics from the identified facial region are retrieved.
- The characteristics include mean skewness or blurred values of Hue, Saturation, and the Variance components, as well as specular reflectance measurements. Each person's features are combined to generate a feature collection.
- Four photos from the genuine images are used for each individual.
- In during testing stage, the same techniques are used to create the test picture and extract the characteristics.
- SVM Classification is then used to evaluate the two characteristics and classify the input test picture.
- The system's ultimate output is to determine if the test picture is a genuine image or a forgery.

Results

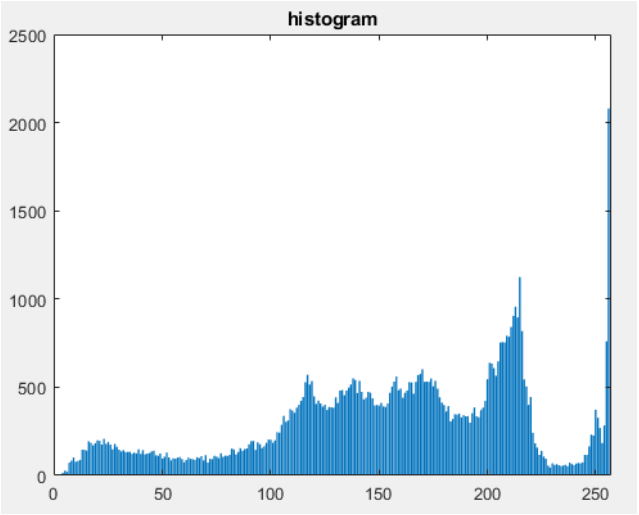
Input Real Image resizing

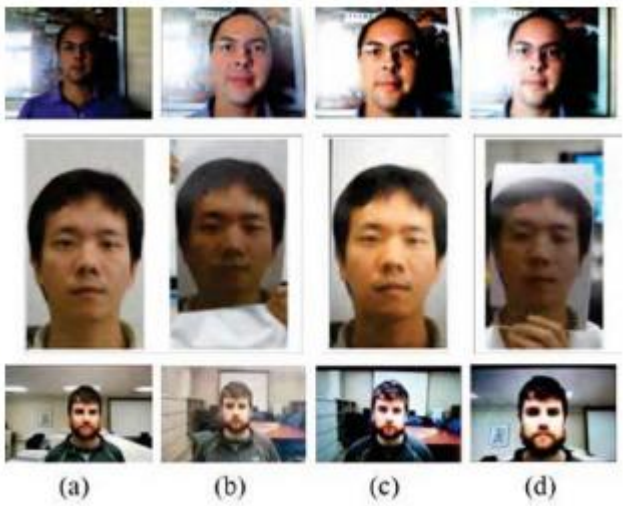
Hue Image Saturation Variance

Detected Region Resizing



Hue Image Saturation Variance



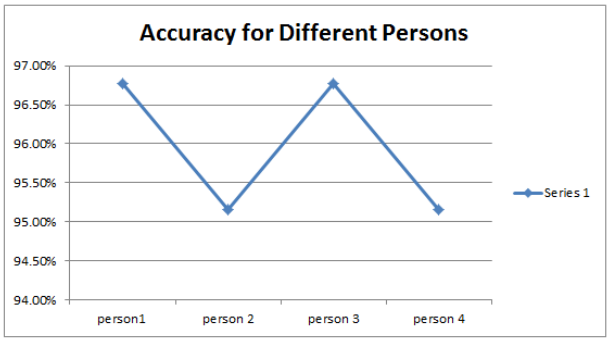


Data base Sample face

Results Accuracy

Person	Accuracy
Person 1	96.7742%
Person 2	95.1613%
Person 3	96.7742%
Person 4	95.1613%

Accuracy Graph



5. Conclusion

Existing biometric systems are vulnerable to spoofing attacks. Spoofing attacks take place when an individual tries to conceal by falsifying data and impersonating another individual. Face printing typically contains print quality flaws that may be discovered using textural characteristics. Thus, we describe a novel method for detecting a living human standing in front of the camera using facial texture analysis. The susceptibility of face recognition technologies to spoofing attacks is generally acknowledged, and this has resulted in considerable advances in anti-spoofing technologies. While progress has been made, facial spoof assaults have proven tough. Furthermore, current approaches for recognising face brightness are employed to detect vitality in a whole face image or video. Image areas, on the other hand, are frequently redundant or correlate to image perplexity, resulting in poor performance. Anti-spoofing facial recognition systems must advance swiftly in order to provide a strong and efficient computing solution to improve the usability of face biometrics. This study proposes a unique paradigm for detecting spoofing in facial recognition systems. To distinguish between the true and faked images, the approach use feature-based analysis. The developed approach is simple and effective in detecting spoofing.

6. Recommendations

The study given here employs basic approaches for detecting the liveness of a face in order to distinguish between a genuine face as well as a spoof face. The system was created utilising photographs of people. One of the possible future developments might be to use video stream as input, which would increase the software's use in a professional setting. Nowadays, many firms, particularly those associated to technology and information technology-enabled activities, have chosen for working at home, resulting in a substantial percentage of the workforce working in such a work from home setting. In this kind of setting, spoof detection may readily monitor the log information and true time involved of the worker. Spoof detecting can also be employed in conjunction with other security and monitoring systems to improve their efficacy. Another area for development is the use of methods for machine learning in conjunction with the existing methodologies.

References

[1] Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. IEEE Transactions on Information Forensics and Security, 10(4), 746-761.

[2] Das, T. R., Hasan, S., Sarwar, S. M., Das, J. K., & Rahman, M. A. (2021). Facial spoof detection using support vector machine. In Proceedings of International Conference on Trends in Computational and Cognitive Engineering (pp. 615-625). Springer, Singapore.

[3] Chinchu, S., Mohammed, A., & Mahesh, B. S. (2017, July). A novel method for real time face spoof recognition for single and multiple user authentication. In 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) (pp. 376-380). IEEE.

[4] Agarwal, A., Singh, R., & Vatsa, M. (2016, September). Face anti-spoofing using haralick features. In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)* (pp. 1-6). IEEE.

[5] Zhang, L. B., Peng, F., Qin, L., & Long, M. (2018). Face spoofing detection based on color texture Markov feature and support vector machine recursive feature elimination. *Journal of Visual Communication and Image Representation*, *51*, 56-69.

[6] Hasan, M. R., Mahmud, S. H., & Li, X. Y. (2019, May). Face anti-spoofing using texture-based techniques and filtering methods. In Journal of Physics: Conference Series (Vol. 1229, No. 1, p. 012044). IOP Publishing.