# MULTIMEDIA SECURITY SPOOFING OF DIGITAL IMAGE FORENSICS -3D FACE MASK

Merlin Livingston L.M.
Associate Professor , ECE Dept., Jeppiaar Institute of Technology, Chennai
Agnel Livingston L.G.X
Assistant Professor ,CSE Dept., St.Xaviers Catholic college of Engineering,Nagercoil
Jenila Livingston L.M.
Associate Professor,SCSE &Learning and research cell,VIT,CHennai

**Abstract:** Biometrics systems have significantly improved person identification and authentication, playing an important role in personal, national, and global security. However, these systems might be deceived (or "spoofed").The recent advances in spoofing detection, current solutions often rely on S domain knowledge, specific biometric reading systems, and attack types. We assume a very limited knowledge about biometric spoofing at the sensor to derive outstanding spoofing detection systems for iris, face and fingerprint modalities. Multimedia Security spoofing is the act of masquerading as a valid user by falsifying data to gain an illegitimate access. Identification of the spoofing performance of the Tampered or Modified Images 2D Data, Video Images, 3D Face Mask and Morphed Location is proposed. The spoofing performance is further analyzed using Opposite Colour Local Binary Pattern (OCLBP) texture based counter measures using 2D data and is further classified using Support Vector Machine (SVM) classifier.

**Key words:** OCLBP,SPOOFING,FANTA MORPH



## I. INTRODUCTION

Biometric human characteristics and traits can successfully allow people identification and authentication and have been widely used for access control, surveillance, and also in national and global security systems [1]. In the last few years, due to the recent technological improvements for data acquisition, storage and processing, and also the scientific advances in computer vision, pattern recognition, and machine learning, several biometric modalities have been largely applied to person recognition, ranging from traditional fingerprint to face, iris, and, more recently, to vein and blood flow. Simultaneously, various spoofing attacks techniques have been created to defeat such biometric systems.

Kevin W. et. al.[2] proposed a method using Near Infrared Illumination (NIR) method. NIR method is Night Vision – sensitive to invisible illumination. .NIR is used in conjunction with an infrared reflection illuminator. Cosmetic contact lenses in iris images is a very difficult pattern-recognition problem.

Nesli Erdogmus . et. al [3] proposed a method using two databases, (i) 3D Mask Attack Database (3DMAD), (ii) LBP-based counter measures for spoofing. Local binary pattern is test relation between pixel and its neighbour's pixels. Then it encodes this relation into binary word. Mainly focusing on 2D attacks forged by displaying printed photos or replaying recorded videos on mobile devices, a significant portion of these studies ground their arguments on the flatness of the spoofing material in front of the sensor. It inspects the spoofing potential of subject-specific 3D facial masks for 2D face recognition. This method introduces the 3D Mask Attack Data base (3DMAD), the first publicly available 3D spoofing database, recorded with a low-cost depth camera. Extensive experiments on 3DMAD show that easily attainable facial masks can pose a serious threat to 2D face recognition systems and LBP is a powerful weapon to eliminate it.

Mayank Vatsa. et. al [4] proposed a method using two databases, namely, the Indian Institute of Technology-Delhi (IIT-D) Iris Contact Lens database and the Notre Dame (ND)-Contact Lens database and prepared to analyze the variations that caused due to contact lenses. The presence of a contact lens, particularly a textured cosmetic lens, poses a challenge to iris recognition as it obfuscates the natural iris patterns. The main contribution of this method is to present an in-depth analysis of the effect of contact lenses on iris recognition. This approach presents a novel lens detection algorithm that can be used to reduce the effect of contact lenses. The proposed approach outperforms other lens detection algorithms on the two databases and shows improved iris recognition performance.

Christian Rathgeb. et. al [5] proposed a modified hill-climbing attack to iris biometric systems. This method demonstrates that reconstructing approximations of original iris images which is highly non-trivial.

Ana F. Sequeira. et. al [6] proposed biometric systems based on iris are vulnerable to several attacks, particularly direct attacks consisting on the presentation of a fake iris to the sensor. The development of iris liveness detection techniques is crucial for the deployment of iris biometric applications in daily life especially in the mobile biometric field. The first Mobile Iris Liveness Detection Competition (MobILive) was organized in the context

of IJCB2014 in order to record recent advances in iris live ness detection. The goal for MobILive was to contribute to the state of the art of this particular subject. This competition covered the most common and simple spoofing attack in which printed images from an authorized user are presented to the sensor by a non-authorized user in order to obtain access.

Pinto et al. [7] proposed research on video-based face spoofing detection. They proposed visual rhythm analysis to capture temporal information on spoofing attacks. The proposed method identifies whether the image is modified or not, but this proposed system presents the details regarding the percentage of morphing.To analyze various texture based counter measures using both 2D & 3D data, a parallel study with comprehensive experiments is performed on two data sets. i.The Morpho database which is not publicly available and ii.The newly distributed 3D mask attack database. This system uses two approaches, (i) Architecture optimization (ii) Filter optimization.

The architecture optimization [8] searches good architectures of conventional networks and adapts the architecture to find the problem in hand. Filter optimization is used to determine filter values with help of back propagation algorithm and discriminates fake and real biometric samples. Back propagation algorithm[9] is used to detect gradient of the loss function.



In existing system, Gray image is taken as the input. So the pixel values will be lost.

Algorithm used is LBP, that applied only for gray scale images and there is no information about the input image morphing.

This paper describes a ELBP algorithm which takes the colour image as input to nullify the drawback of the existing system. As the input is colour image, the pixels values are not altered. The existing system identifies whether the image is modified or not, but this proposed system presents the details regarding the percentage of morphing.

## II. PROPOSED SYSTEM

This paper is developed in order to detect the illegal access on face. Here the face recognition is classified into 1) Image acquisition 2) Morphing 3) Processing of images using ELBP algorithm that run MATLAB 4) Classification using SVM.

In the first module, the acquisition of images can be done from databases. In the second module, the acquired images can be morphed with the help of Fanta morph software. In the third module, the original image as well as the morphed image can be given to the Extended Local Binary Pattern (ELBP) algorithm which performs spoofing detection. ELBP algorithm compares the centre pixels with the neighborhood pixels and finds the relationship of pixels then encodes the relationships into binary word. Last module, perform classification with the help of Support Vector Machine (SVM) classifier which says whether the image is modified or not and also finds the location of the morphed and percentage of the morphing.

Colour image is taken as input to the system, so that the pixel values are not altered. Hence authentication of images are more secured. In existing system only gray scale image is taken as an input. The operator has been developed to analyses the pattern both in gray scale and the colour domain By ELBP algorithm. The operator is based on the human vision to interpret colour as opponent colours such as red-green or blue – yellow. This system is applied to identify morphing or tampering in images, videos and 3D face mask.



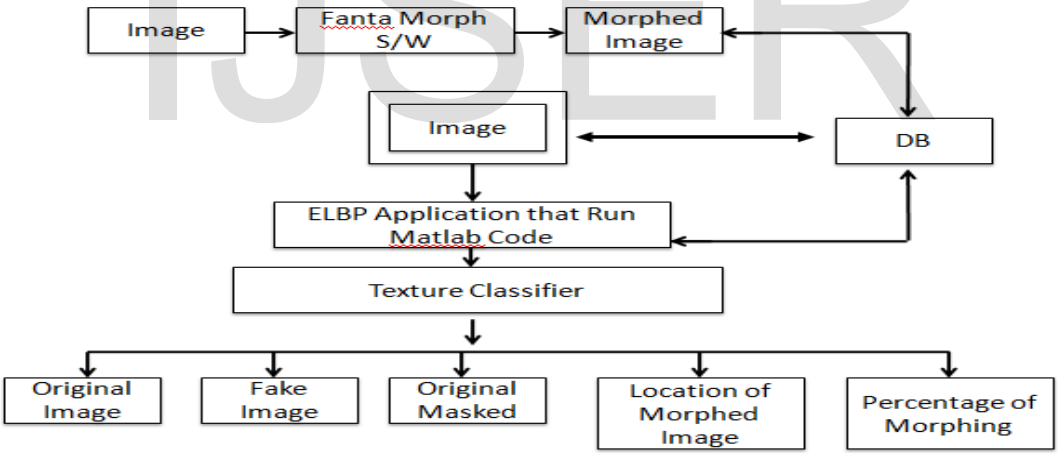


**Figure 1. Block Diagram**

The image which is going to be morphing is given to the (Fanta morph software) second block. In this block the image will be morphed by Fanta morph software where the required morphed image will be obtained. The corresponding morphed image is given to the data acquisition board which contains number of original images. The output image from the third block is compared with the data acquisition board. This process takes place in fourth block. The ELBP algorithm again compares the output of fourth block with the help of MATLAB code.

This output is given to the SVM classifier. The support vector machine classifier will classify whether the image is original, fake or morphed and it also finds the location of morphing and percentage of morphing.

## III. SYSTEM DESCRIPTION

Acquisition is the first essential step for entire process. Image acquisition in image processing can be broadly defined as the action of retrieving an image from some source. Performing image acquisition in image processing is always the first step in the workflow sequence, because without an image, no processing is possible. The image that is acquired is completely processed and is the result of whatever hardware was used to generate it, which can be very important in some fields to have a consistent baseline from which to work. One of the ultimate goals of this process is to have a source of input that operated within controlled and measured guidelines.



### LOGITECH QUICK CAM

This Logitech quick cam is used for image acquisition process. This device that originally shiped with the camera included Quick Movie for recording motion pictures and Quick PICT for capturing still images. It produced 16 shades of gray at a resolution of 320×240 pixels, and could record video at about 15 frames per second. It cost $ 100. Today, Logitech Quick Cam is one of the world's most recognized webcam brands.

**(a) Input image 1**

**(b) Input image 2**

**Figure 2 (a),(b):Input Images**

A major factor involved in image acquisition is the initial setup and long term maintenance of the hardware used to capture the images. Here the Logitech quick camera can be used to capture the images. The actual hardware device can be anything from a desktop scanner to a massive optical telescope. If the hardware is not properly configured and aligned, then visual artifacts can be produced that can complicate the image processing. One of the forms of image acquisition in image processing is known as real time image acquisition. This usually involves retrieving images from a source that automatically captures images. Real time image acquisition creates a stream of files that can be automatically processed, queued for later work, or stitched into a single media format.

**IMAGE MORPHING:**

**Figure 3 Morphed image**

In image morphing, the images can be acquired from the previous step. Both images can be morphed with help of Fanta Morph software. Image from the image acquisition process is not always same in size. To perform morphing easily resize code is used to get the same size image.

**ELBP ALGORITHM FOR SPOOFING**:

ELBP-Extracted Local Binary Pattern is an algorithm to differentiate original image and morphed image. LBP[10] is a type of visual descriptor used for classification in computer vision.

## LBP operation:

i. Divide image into cell(16*16 for each cell).

ii. For each pixel in a cell, compare the pixel to each of its 8 neighbors(on its left top, left middle, left bottom, right top) follow the pixels along a circle i.e. clockwise or counter clockwise

iii. Where the centre pixel's value is greater than the neighbour's value, write "0". Otherwise, write "1". This gives an 8 digit binary number which is usually converted to decimal for convenience.

iv. Compute the histogram, over the cell, of the frequency of each "number" occurring.

v. Concatenate histograms of all cells. This gives a feature vector for the entire window.



This feature vector can be processed using the support vector machine to classify the images. Such classifiers can be used for face recognition or texture analysis.The existing methods such as Liveness detection and motion analysis failed in detection of 3D mask attacks. So, the proposed system approaches texture analysis method . Human skin differs from mask material with its optical characteristics, such as reflectance, scattering etc. makes it possible to use texture properties to discriminate between real accesses and spoof attacks. Normally LBP is used for gray scale images. ELBP algorithm is suitable for both gray and colour images. When we used gray scale image as an input, the pixel values are altered. Hence, the pixel values are secured.

SVM classifier is used to classify the different outputs. SVM determines whether the image is original or fake and presents details on location and the percentage of morphing. The main advantage of SVM classifier is that can be used for nonlinear classification.

## IV. CONCLUSION

Now a days, the rate of illegal access through which people buy High Quality Fake and Unregistered Visa, Passport , ID card, Birth Certificate, Driver's License, Transcripts, National and International Certificates, Social Security Cards, Medical Certificates, Football Licenses, Residence Permits and many more others is rapidly increasing. In order to detect this illegal access spoofing technique is used in this paper. We have evaluated the identification of tampered face. The spoofing performance is analyzed using Opposite Colour Local Binary Pattern texture based counter measures using 2D data and is classified using Support Vector Machine classifier. This paper mainly focuses on 3D Face Mask.

**FUTURE WORK**

Even though the system is very accurate, it focuses only on detection of spoofing on face. It is very essential to develop the system which is built on more biometric traits. So, it would be better if there is an additional biometric traits like voice or signature. Using the same classifier, the work has to be extended till the system is compatible most of the biometric traits for the maximum accuracy. By doing this, we can further increases the performance of a system.



## REFERENCES

[1] A. K. Jain and A. Ross, (2008) Handbook of Biometrics. Springer, ch.Introduction to biometrics, pp. 1–22.

[2] K. W. Bowyer and J. S. Doyle,( 2014) “Cosmetic contact lenses and iris recognition spoofing,” Computer, vol. 47, no. 5, pp. 96–98.

[3] N. Erdogmus and S. Marcel, (2013) “Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect,” in IEEE Int. Conference on Biometrics: Theory Applications and Systems (VISAPP), pp. 1–6.

[4] M. Vatsa, D. Yadav, N. Kohli, J. Doyle, R. Singh and K. Bowyer,( 2014)“Unraveling the effect of textured contact lenses on iris recognition,”IEEE Trans. Inf. Forens. Security, vol. 9, no. 5, pp. 851–862.

[5] C. Rathgeb and A. Uhl,( 2010) "Attacking iris recognition: An efficient hillclimbing technique," in IEEE/IAPR International Conference on Pattern Recognition (ICPR), pp. 1217–1220.

[6] A. F. Sequeira, J. C. Monteiro, H. P. Oliveira, and J. S. Cardoso,(2014) "MobILive 2014 - Mobile Iris Liveness Detection Competition," in IEEE Int. Joint Conference on Biometrics (IJCB).

[7] A.Pinto, H. Pedrini, W. R. Schwartz, and A. Rocha, (2012)"Video-based face spoofing detection through visual rhythm analysis," in Conference on Graphics, Patterns and Images (SIBGRAPI), pp. 221–228.

[8] J.Bergstra and Y. Bengio,( 2012) "Random search for hyper-parameter optimization,"Journal of Machine Learning Research, vol. 13, pp. 281–305.

[9] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner,(2009) "Gradient-based learning applied to document recognition," Proceedings of the IEEE, vol. 86,no. 11, pp. 2278–2324.

[10] I. Chingovska, A. Anjos, and S. Marcel (2012) "On the effectiveness of local binary patterns in face anti-spoofing," in Int. Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–7.