A Paper on Face Recognition with Visible and Thermal Infrared Imagery

1Shyam Lal, 2Dr. Naveen Sharma
1M.Tech (CSE), 2HOD
1,2ICL Institute of Engineering and Technology, Ambala
1oreoshyam574@gmail.com, 2Naveen.sharma@iclhitech.com

Abstract: We present a comprehensive performance study of multiple appearance-based face recognition methodologies, on visible and thermal infrared imagery. We compare algorithms within the same imaging modality as well as between them. Both identification and verification scenarios are considered, and appropriate performance statistics reported for each case. Our experimental design is aimed at gaining full understanding of algorithm performance under varying conditions, and is based on Monte Carlo analysis of performance measures. This analysis reveals that under many circumstances, using thermal infrared imagery yields higher performance, while in other cases performance in both modalities is equivalent. Performance increases further when algorithms on visible and thermal infrared imagery are fused. Our study also provides a partial explanation for the multiple contradictory claims in the literature regarding performance of various algorithms on visible data sets.

Keywords: face recognition; thermal image; noise influence;

I. INTRODUCTION

One of the major disadvantages of visible light face recognition systems is illumination dependency. In order to overcome this problem, the use of passive thermal infrared sensors, which measure emitted heat energy from object, is increased in the most critical security systems for verification and authentication. The main advantage of thermal spectrum is a fact that thermal sensors collect the energy emitted by an object which is not affected with illumination changes. Moreover, thermal images can provide enough useful information for successful face recognition methods even in conditions of complete darkness. As our everyday life is getting more and more computerized, automated security systems are getting more and more important. Today most personal banking tasks can be performed over the Internet and soon they can also be performed on mobile devices such as cell phones and PDAs. The key task of an automated security system is to verify that the users are in fact who they claim to be.

Facial recognition analyzes the characteristics of a person’s face images input through a digital video camera. It measures the overall facial structure, including distances between eyes, nose, mouth, and jaw edges. These measurements are retained in a database and used as a comparison when a user stands before the camera. This biometric has been widely, and perhaps wildly, touted as a fantastic system for recognizing potential threats (whether terrorist, scam artist, or known criminal) but so far has been unproven in high-level usage. It is currently used in verification only systems with a good deal of success.

<table>
<thead>
<tr>
<th>Methods</th>
<th>Examples</th>
<th>Problems</th>
</tr>
</thead>
<tbody>
<tr>
<td>What we know</td>
<td>Password, PIN, ID</td>
<td>Forgotten, Shared, Easy to guess</td>
</tr>
<tr>
<td>What we have</td>
<td>Key, Cards etc.</td>
<td>Lost or Stolen, Can be duplicated</td>
</tr>
<tr>
<td>What we are</td>
<td>Fingerprint, Face, Iris etc.</td>
<td>Non-repudiable authentication</td>
</tr>
</tbody>
</table>

Table I. Identification Technologies

Fig 1. Enrollment Process in Biometrics System

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an
In this technique, the user faces the camera, standing about two feet from it. The system will locate the user's face and perform matches against the claimed identity or the facial database. It is possible that the user may need to move and reattempt the verification based on his facial position. The system usually comes to a decision in less than 5 seconds.

Biometric is necessary due to these characteristics:

- Links the event to a particular user (a password or symbol may be used by somebody other than the approved user)
- Is convenient (nothing to carry or memorize)
- Accurate (it provides for positive authentication)
- Fast and scalable
- Easy to use and easily understandable
- Is becoming socially acceptable and
- Cost effective

II. FACE RECOGNITION TECHNIQUES

A. Liveness Detection in Biometric System: Liveness detection is a measure that determines whether or not the source of the image presented to a biometric sensor is from a living individual or not. Liveness detection technique is now become a most important part for any biometric system. There are various biometric system which requires different types of biometric trait for authentication purpose, e.g. fingerprint recognition, iris recognition, face recognition etc.

B. Fake Face Recognition using Fusion of Thermal Imaging and Skin Elasticity:-

Face recognition is a process of identifying and verifying a person by recognizing his face. Face recognition has become an important issue in many applications such as security systems, credit card verification, criminal identification etc. Due to recent pattern recognition advances applied to face recognition, biometric systems based on facial characteristics have been largely applied to problems, including access control, surveillance and criminal identification.

III. PROPOSED ALGORITHMIC APPROACH

In this technique thermal camera is fitted at predetermine distance from the visible camera. Images are captured at the same time from both the camera by specified instruction. For skin elasticity process a set of image sequence is captured with a gap of few milliseconds. The steps are as below.

Step 1. Request the user to perform live activities like chewing, smile, forehead movement etc.
Step 2. Now at the same time capture a sequence of face images with a gap of few milliseconds and a thermal image using low IR thermal imaging camera.
Step 3. Now select one of the image from the set of image sequence to compare with thermal image in such a way it is captured at the same time.
Step 3. Now perform grey scale method on both selected images.
Step 4. Now convert both resulted images into binary image using binary scaling method.
Step 5. According to distance of thermal camera from the visible image camera perform angular deviation on thermal image after thinning on both images.
Step 6. Now superimpose matching on both images and calculate the matching percentage.
Step 6. If calculated value is greater than the threshold value then the image captured are real time images. And if parallely, skin elasticity test on the set of image sequence is passed then image captured are from real person without any fake face.
Step 7. If at any one stage the process fails then complete process fails and resulted into fake image analysis.

Advantages of fusion of these two liveness detection techniques are following:
1. Thermal imaging is capable of identifying fake face and images captured from photo or video
2. Skin elasticity is capable of distinguishing fake faces that uses gelatin, rubber, clay etc. material.
3. Using both these techniques we will be capable of identifying real face from fake faces.
4. Other Advantages of this approach is that it is user friendly approach.
5. Since it involve thermal imaging camera (Hardware) technique and skin elasticity technique (software based method), so we need not to rebuild the face database.
6. One image of the set of image sequence can be used for face recognition.

IV. CONCLUSION
In this paper we Face recognition has received substantial attention from researches in biometrics, pattern recognition field and computer vision communities. Using neural network as a classifier we can increase recognition rate, acceptance rate and decrease the execution time as shown by study done by different researchers. Moreover, we describe the most common mechanisms of discretionary security and stated the emerging security used in distributed system tools.

In future, face recognition can combine genetic algorithm with neural network to increase the acceptance rate, recognition rate and execution time while using low resolution images. There is a lot of work required in this field to use the liveness detection easily and broadly with high acceptance rate. In future the techniques mention in this dissertation can be experimented at practical level on set of large data.

REFERENCES