Chapter 8
Robotics and Multimodal Biometrics

ABSTRACT

This chapter presents a review on a new subfield of security research which transforms and expands the domain of biometrics beyond biological entities to include virtual reality entities, such as avatars, which are rapidly becoming a part of society. Artimetrics research at Cybersecurity Lab, University of Louisville, USA, and Biometric Technologies Lab, University of Calgary, Canada, builds on and expands such diverse fields of science as forensics, robotics, virtual worlds, computer graphics, biometrics, and security. Analyzing the visual properties and behavioral profiling can ensure verification and recognition of avatars. This chapter introduces a multimodal system for artificial entities recognition, simultaneously profiling multiple independent physical and behavioral characteristic of an entity, and creating a new generation multimodal system capable of authenticating both biological (human being) and non-biological (avatars) entities. At the end, this chapter focuses on some future research directions by discussing robotic biometrics beyond images and text-based communication to intelligent software agents that can emulate human intelligence. As artificial intelligence and virtual reality domains evolve, they will in turn give rise to new generation security solutions to identity management spanning both human and artificial entity worlds.

1. INTRODUCTION

Over the course of history, the greatest minds: scientists, philanthropists, educators, politicians, leaders, philosophers, were fascinated with the way human brain works. From Michelangelo to Lomonosov, from DaVinci to Einstein, there have been numerous attempts to uncover the mystery of human mind and to replicate its working first through simple mechanical devices an later, in the 20th century, through computing machines, software and robots.

DOI: 10.4018/978-1-4666-3646-0.ch008

In Alan Turing's 1950 work "Computing Machinery and Intelligence," Turing posed the question "can machines think?" In order to establish credible criteria to answer this question, he proposed a test, now known as "The Turing Test"—to evaluate a machine's ability to demonstrate intelligence. At the core of the test is conversation in a natural language between the human judge and the opponent, who can be either human or a machine. If the judge cannot reliably tell the machine from the human, the machine is said to have passed the test. In the light of recent developments, it can be viewed as the ultimate multimodal behavioral biometric, which can detect differences between a man and the machine.

Following Turing's work, another foundation of modern artificial intelligence was laid out by John von Neumann in the 1950s in his theory of automata and self-replicating machines. His theoretical concepts were based on those introduced by Alan Turing. The majority of research in this domain is focused on self-replicating programs and systems. Thus, development of computer viruses and spam e-mail applications has been quite fruitful. The obvious difficulty challenge lies with making robots reproduce themselves.

Self-replication in biological world is fairly well understood. The process of self-replication at the molecular level is responsible for all the living organisms on Earth today. Self-replication of non-biological entities is much less understood process. Much attention was devoted to the Cornell University researchers who have created a machine that can build copies of itself. Their robots are made up of a series of modular cubes—called "molecubes"—each identical to each other and each supplied with computer program for replication. The complete robot is built from a number of cubes, which connect by using electromagnets.

However, the bigger question of authentication and labeling of such "self-replicating" robots and software (such as viruses) has rarely been posed, despite the growing concerns that uncontrollable development of self-replicating machines and machines with artificial intelligence can be somewhat harmful for the human society. And examples are numerous. Domestic and industrial robots, intelligent software agents, virtual world avatars and other artificial entities are quickly becoming a part of our everyday life. Just like it is necessary to be able to accurately authenticate identity of human beings, it is essential to be able to determine identity of the non-biological entities (Gavrilova & Yampolskiy, 2012). Military soldier-robots (Khurshid & Bing-Rong, 2004), robots museum guides (Charles, Rosenberg, & Thrun, 1999), software office assistants (Chen & Barthes, 2008), human-like biped robots (Lim & Takanishi, 2000), office robots (Asoh, Hayamizu, Hara, Motomura, Akaho, & Matsui, 1997), bots (Patel & Hexmoor, 2009), robots with human-like faces (Kobayashi & Hara, 1993), virtual world avatars (Tang, Fu, Tu, Hasegawa-Johnson, & Huang, 2008) and thousands of other man-made entities all have something in common: a pressing need for a decentralized, affordable, automatic, fast, secure, reliable, and accurate means of identity authentication. To address these concerns, the concept of *Artimetrics* – a field of study that will allow identifying, classifying and authenticating robots, software and virtual reality agents has been proposed in (Yampolskiy, 2007a; Yampolskiy & Govindaraju, 2007; Gavrilova & Yampolskiy, 2012).

While the area of robot and agent authentication may seem a bit futuristic at first, careful analysis of recent news stories shows that this is not quite so. To give just some examples: terrorists have been reported recruiting and communicating in virtual communities such as Second Life (Cole, 2008). Cybercrime, including identity theft, is rampant in virtual worlds populated by millions of avatars and operating multibillion dollar economies (Nood & Attema, 2009). Security experts