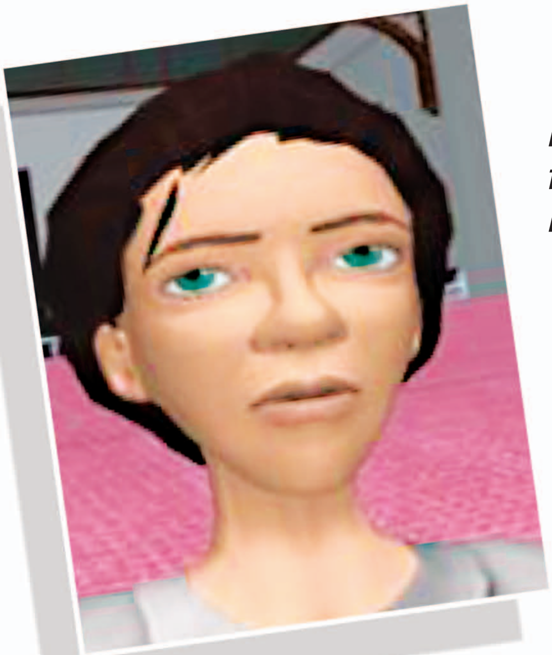
Artimetrics

Biometrics for Artificial Entities

By Roman V. Yampolskiy and Marina L. Gavrilova

Domestic and industrial robots, intelligent software agents, virtual-world avatars, and other artificial entities are being created and deployed in our society for various routine and hazardous tasks, as well as for entertainment and companionship. Over the past ten years or so, primarily in response to the growing security threats and financial fraud, it has become necessary to accurately authenticate the identities of human beings using biometrics. For similar reasons, it may become essential to determine the identities of nonbiological entities. Trust and security issues associated with the large-scale deployment of military soldier-robots [55], robot museum guides [22], software office assistants [24], humanlike biped robots [67], office robots [5], domestic and industrial androids [93], [76], bots [85], robots with humanlike faces [60], virtual-world avatars [109], and thousands of other man-made entities require the development of methods for a decentralized, affordable, automatic, fast, secure, reliable, and accurate means of authenticating these artificial agents. The approach has to be decentralized to allow authority-free authentication important for open-source and collaborative societies. To address these concerns, we proposed [117], [120], [119], [38] the concept of *artimetrics*—a field of study that identifies, classifies, and authenticates robots, software, and virtual reality agents. In this article, unless otherwise qualified, the term *robot* refers to both embodied robots (industrial, mobile, tele, personal, military, and service) and virtual robots or avatars, focusing specifically on those that have a human morphology.

Virtual worlds populated by software robots are an area of particular concern [123]. A quick investigation of the Second Life virtual world shows that it is populated by organizations posing security



Digital Object Identifier 10.1109/MRA.2012.2201574

Date of publication: 6 December 2012

1070-9932/12/$31.00©2012IEEE

risks, including international terrorist groups and local groups of radicals. Virtual worlds can be used to create an exact replica of a real-world target and can be utilized to rehearse an entire attack online, including monitoring the response and ramifications [78]. We can further illustrate the problem by analyzing the examples of news reports about the crimes reported to be committed in the virtual communities. These crimes are either committed by members of the virtual communities through their avatars or directly by creating malicious software that can accomplish committing the crime. In either case, "as in the real world, one of the central difficulties is establishing the identity of individuals" [79]. The examples given below are by no means exhaustive, because almost any type of real crime has a virtual equivalent [123]

1) *Theft of Virtual Property*—"The Netherlands teen sentenced for stealing virtual goods" [33]
2) *Virtual Prostitution, Strip Clubs, and Pornography*—"Escorts, the Second Life equivalent of phone-sex operators or prostitutes, are quite common in Second Life" [115]
3) *Virtual Gambling*—"FBI checks gambling in Second Life virtual world" [84]
4) *Virtual Money Laundering*—"Second Life and other online sites targeted by criminals" [105]
5) *Virtual Fraud*—"…the 'bank' vanished, and depositors say their money did, too" [106]
6) *Identity Theft*—"Second Life charges for real names, increases identity theft risk" [113]
7) *Illegal Content (Child Porn)*—"Second Life 'child abuse' claim" [9].

In addition to numerous examples of virtual crime, it is also interesting to look at other scenarios in which it would be useful to track an individual between the real and virtual worlds. For example, a number of cases have been reported in which a wanted criminal is easily found in the virtual world and even taunts authorities by posting status updates and pictures of his real environment [97], [111].

In the context of investigating criminal and terrorist activity outlined above, we see six (four nonsymmetrical) scenarios requiring an automated matching algorithm (see Figure 1). For each scenario, we have provided a realistic example meant to motivate the need for a particular matching algorithm [123].

1) *Matching a human face to an avatar face and vice versa* [Figure 1(a)]: This capability is useful to connect a person's real identity to their virtual persona. It is increasingly common to upload a real photograph to serve as a prototype for a 3-D avatar, as well as to create drawings closely resembling the actual person to serve as the online persona.

   Example scenario 1 (avatar to human): During a forensic investigation of a personal computer, a number of images depicting virtual pornography are found. It is desirable to run the virtual faces against the database or real-life sex offenders to see whether any quality matches can be detected for further investigation.

   Example scenario 2 (human to avatar): To follow up a convicted sex offender forbidden from interactions with anyone under 18, it might be valuable to do a visual search of virtual playgrounds to see whether the person is violating the court order in cyberspace.

2) *Matching the face of one avatar to another avatar* [Figure 1(b)]: This capability is useful for continuously tracking a virtual persona through cyberspace at different times and in different places.

   Example scenario 1: An intelligence agency might be interested in automatically tracking a suspected terrorist across the virtual community for many days to establish his contacts and frequently visited places.

   Example scenario 2: The same capability might be extremely useful in personalization and customization of services, for example, to load certain user preferences if a recognized avatar returns to a previously visited business.

   Example scenario 3: The ability to recognize avatars and profile them on the basis of appearance is also very useful in marketing; for example, a cosmetics company selling their product in a virtual world might be interested in advertising to all female avatars who appear to use a lot of lipstick.

3) *Matching an avatar's face from one virtual world to the same avatar represented in a different virtual world(s)* [Figure 1(c)]: A recent development in the world of virtual communities is the desire to interconnect different virtual worlds. "One such world, called HiPiHi, is being created in China. HiPiHi founders said they want to create ways for avatars to travel freely between its virtual world, Second Life and other systems—a development that intelligence officials say make it doubly hard to track down the identity of avatars" [79].

   Example scenario: A well-known criminal has set up recruitment camps in multiple virtual worlds (Second Life, Entropia Universe, etc.). To fully understand his minute-by-minute activity, network of contacts, and overall strategy, it is necessary to track him beyond a single virtual world to all corners of the cyberspace. Because the same real-world photograph will be translated to slightly different-looking avatars depending on the algorithm used by a specific virtual world, it is very

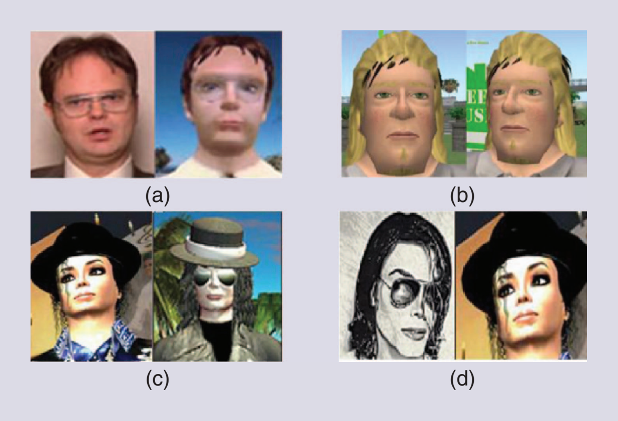


Figure 1. Four possible avatar-matching scenarios useful in forensic investigations [123]. Images from (a) cyberextruder.com, (b) SecondLife.com, (c) SecondLife.com and EntropiaUniverse.com, and (d) RedFieldPlugins.com.

valuable to do intervirtual world avatar tracking via avatar-to-avatar matching.

4) *Matching a sketch of an avatar to an avatar's face and vice versa* [Figure 1(d)]: Because it is useful to match a sketch created on the basis of the description provided by a victim or a witness of a crime to a picture of a criminal from an FBI database, it is also important to match a sketch of a virtual criminal to an actual avatar responsible for the crime.

Example scenario 1 (sketch to avatar): In the case of a virtual crime [68], the victim may not know the identity of the avatar responsible but will probably provide a verbal description of the assailant from which a sketch artist will generate a fairly close representation of the wanted avatar. Given such a sketch, it is desirable to have the technological ability to scan through a dataset of avatars in the given virtual community and find avatars, which are best matches for the sketch.

Example scenario 2 (avatar to sketch): In a scenario similar to the one above, if a database of all the avatars in the world is not available, a wanted poster approach might be utilized. In this approach, a sketch of the wanted criminal is made public in the virtual world, and avatars passing by can compare their acquaintances to the depiction on the wanted poster.

With continued progress in software and hardware robotics and related fields, it is logical to expect the next generation of robots to resemble humans and possess the abilities of humans, including walking, speaking, typing, and making decisions (Figure 2 shows how robots are becoming more humanlike with every generation).

It is also likely that robot owners might choose to customize their robots' appearances, similar to people frequently electing to customize their cell phones or computers via "skins" or desktop wallpapers, which will result in robots being truly unique in appearance. The feature that naturally lends itself to customization is the face; in fact, celebrity look-alike [80] and model robots [47] have already appeared. The robots of tomorrow may also present a security threat to people, property, and cyber infrastructure, depending on who is controlling them and their learned skills. Thus it is a natural progression to extend research in biometrics-based human authentication to methods for recognition of robots.

Biometric authentication is applicable to intelligent robots/software authentication in a number of different instances. Lyons et al. discussed specific steps and processing techniques needed for an avatar to be created almost automatically from the human face [69]. In fact, the process described by Lyons et al. is essentially the process of biometric synthesis [126]. Users of virtual worlds have also noted that avatars very often resemble the characteristics of its creator, not only in facial characteristics but also in body shape, accessories, and clothes.

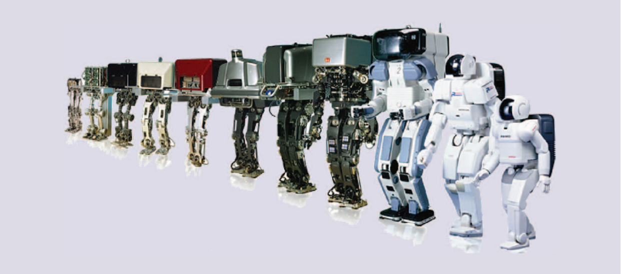


Figure 2. Evolution of the Honda Asimo robot from 1986 to 2000 [46].

But what about other less obvious resemblances such as manner of communication, response to various situations, nature of work, leisure/recreational activities, and time of appearing in the virtual world? All of the above encompass behavioral characteristics or soft biometrics [49] that can be exploited by fusing biometric-based techniques with methodology tailored to the specifics of virtual world. Such behavioral characteristics are even less likely to change than the avatar's facial appearance and clothes during the virtual world sessions, as users typically invest a lot of time and money into the creation of a consistent virtual image and are unlikely to change an avatar's patterns of behavior.

Literature Review

To date, very few works have dealt with the visual or behavioral authentication of robots. The need for the development of robotic biometrics has been identified in [127]. Relevant work has been done in program recognition [83] and program understanding [87] in which the source code of a program is analyzed with the goal of understanding the original purpose behind the creation of such software. Others have researched robot behavior recognition and prediction, never applying the discovered trends to the recognition of robots exhibiting the observed behavior [7], [44]. Finally, work in robot detection [54], [108] and robot self-recognition [53], [40] is closely related and can serve as additional support for the proposed research.

Although no research has been reported in automatic robot authentication or behavior analysis, some relevant research has been published on robot emotion recognition [34]. Canamero and Fredslund conducted a study to evaluate how accurately humans can recognize facial expressions displayed by the humanoid robot Felix. The average recognition accuracy of emotion expressions was 58% for adults and 64% for children. In a control group recognizing emotion in human faces, the results were 82% for adults and 70% for children [18]. The surprising conclusion of this study was that children are better than adults at recognizing robots' emotional states, which could possibly be explained by children's significant exposure to modern cartoons populated by robotic creatures.

In a different set of experiments, Elliot tested the ability of intelligent agents to express emotions by having humans gather enough information from the agents' different communication modalities to correctly assign intended meanings to ambiguous sentences. These agents can interact with subjects using speech recognition, text-to-speech, real-time morphed schematic faces, and music. By comparing the performances of computerized agents to human actors, Elliot showed that artificial agents outperformed humans by 53–70% [32]. In a related set of experiments, Bruce et al. determined the degree to which emotional expression affects a robot's ability to engage with humans [17]. Their robot exhibited different emotions on the basis of its success at recruiting a passerby to take a poll. The results showed that having an expressive face and appropriate movement (body language) increases a robot's chance of successful interactions.

The work of Delaunay et al. [31] focused on understanding how a person in a human-robot interaction can read gaze direction from a robot. Results of their experiments indicate that although it is hard to recreate human-human interaction performance, robot faces having a humanlike physiognomy perform equally well, which seems to suggest that these are the preferred candidates to implement joint attention in human-robot interaction [31]. Saerbeck and Bartneck [92] analyzed the relationship between the motion of a robot and perceived effect on human beings. Acceleration and curvature appear to be the most influential factors in how the motion is perceived. Experimental results suggest a strong relationship between motion parameters and attribution of affect, while the type of embodiment had no effect.

Riek et al. [90] showed that people cooperate with abrupt gestures quicker than with smooth gestures. A person's speed at decoding robot gestures is correlated with his or her ability to decode human gestures, and negative attitudes toward robots are strongly correlated with a decreased ability in decoding human gestures [90]. Chaminade et al. [21] gave instructions to volunteers to explicitly attend to the emotion shown by human and robot subjects. A significant increase was observed in response to robot, but not human facial expressions in the anterior part of the left inferior frontal gyrus, a neural marker of motor resonance [21].

The research on robots exhibiting emotions has a rich history. The following is a short list of robots that demonstrate different levels of facial expressions [18].

Affective Tiger is a toy robot developed as a tool for social and emotional awareness education of young children. Tiger's face has two degrees of freedom (2 DoF) (mouth and eyes) [57].

Minerva is an interactive tour guide robot that displays four emotions: neutral, happy, sad, and angry. It has 4 DoF: two for mouth control and two for the eyebrows [23].

Sparky is a teleoperated robot, which uses facial expressions, gestures, motions, and sounds to interact with people. His face has 4 DoF to control three expressive features—eyebrows, eyelids, and lips [98].

Kismet is a famous MIT robot developed as a testbed for learning social interactions between robots and people. Kismet's face has 18 DoF that allow the robot to express a full range of emotions, which have been shown to be correctly interpreted by people [16].

iCub was designed by a consortium of European institutions to simulate the perceptual system and articulation of a small child and to interact with the world in the same way that a child does. The robot has 53 DoF distributed between its arms (seven each), hands (nine each), head (six), torso (three), and legs (six each) [77].

In addition to experiments on understanding the emotional states of robots, some work has been started on the general analysis of avatar behavior [15]. Another novel research direction is known as Avatar DNA, a patent-pending technology from Raytheon [110]. A recently published article demonstrates the feasibility of applying strategy-based purely behavioral biometrics developed for the recognition of human beings to the recognition of intelligent software agents [122]. The article lays the theoretical groundwork for research in the authentication of nonbiological entities. Specifically, it is demonstrated that behavioral biometrics is a sound approach to intelligent robot authentication.

Artimetrics

Database Generation and Availability

In well-established fields such as biometrics, numerous standardized and publicly available datasets exist [66], making it possible to compare different algorithms and to test developed systems. Labeled public datasets of robot faces, avatars, or attributed conversations from artificially intelligent agents are currently unavailable. A visual survey of robots [38] contains images of various artificial entities but not a standardized database suitable for subsequent research. Methods for synthetic iris, face, and fingerprint database generation for biometric research were recently surveyed [119], [120]. However, for the robot domain, this is mainly an unexplored area of research. Techniques for the creation of such standardized datasets that are consistent with real-world datasets can be imitated by examining the approaches to the generation and evaluation of facial datasets [59], [37] utilized by biometric systems or from chat mining research applied to gender attribution and human versus bot classification [27], [39].

The authors have begun to work on the generation of a publicly available avatar face dataset [82], and on the collection of speech corpora from intelligent agents—two types of data, which are of specific interest in the early artimetrics research. One database consists of a set of high-resolution facial images of avatars collected from two of the most popular virtual worlds: SecondLife.com and EntropiaUniverse.com. The other database consists of a text corpus from intelligent agents who have performed extremely well in the recent Loebner Prize in Artificial Intelligence (AI) competitions (Loebner.net). We have developed automated tools utilizing the power of AutoItScript.com and the Linden scripting language (LindenLab.com) for the creation of customized datasets of both kinds. With the assistance of the developed tools, researchers in the field can effortlessly generate virtually unlimited amount of data for visual and stylometric robot authentication experiments. Additional work is still necessary to make it possible to generate data with specific characteristics. Currently, it is only possible to specify the desired amount of data, the gender of the avatars' faces, and the overall area of knowledge over which the intelligent agents communicate. It is, however, already possible to generate multiple samples for each nonbiological entity, making it easy to perform training and testing on disjoint datasets. In parallel, we are working on assembling a dataset of hardware robots' faces, a process which, due to the current limited number of such robots, is done manually and provides limited control over such factors as DoF in facial expressions (see Figure 3). First evaluation results on such synthetic databases have appeared in the literature [130], [118], [13], [3], and the achieved accuracy rates are comparable to those achieved on human face datasets. The difficulties faced by artimetrics researchers are similar to those in the field of biometrics, such as chaotic and noisy environments, varied lighting conditions, subject occlusion, and system spoofing by well-trained adversaries.

Visual Artimetrics

1) *Goals:* Authentication of robots can be carried out through some methodologies developed for authenticating human beings in the field of biometrics and in others dealing with the attribution of identity, such as authorship recognition or stylometry (as practiced in forensic science). Biometrics is defined as the science of human identity authentication via analysis of measurable physiological and behavioral characteristics [49], [50]. With respect to authentication, face recognition is one of the most popular physical biometrics, which can also be applied to authentication of humanoid robots. Prior research related to *visual authentication* of identity on the basis of face analysis that can be applied to robot authentication is summarized below.

2) *Methods:* Face detection is the first step in the authentication process in which a face is located in an image to make further processing possible. A very large number of articles have been published on the topic; interested readers are referred to survey articles [125], [129], [107] as well as a recent book [48] on facial biometrics. Dozens of different approaches ranging in accuracy from 60% to 99% have been proposed [125]. They are generally classified as knowledge-based, feature-invariant, template-matching, and appearance-based. Knowledge-based methods, such as the multiresolution-based approach [124], capture the relationship between facial features. Feature-invariant approaches look for the structure's consistency under a variety of poses and lighting conditions; examples include grouping of edges [128], a space gray-level dependence matrix [30], and a mixture of Gaussians [70]. The template-matching method extracts standard patterns of the face, which are later compared to regions being tested to determine the degree of correlation; classical examples include a shape template [29] and active shape model [64]. Finally, appearance-based methods, such as Eigenvector decomposition [112], support vector machines (SVMs) [81], the hidden Markov model [89], the naive Bayes classifier [99], and neural networks [91] learn facial templates from a set of training images.

3) *Pros and Cons:* Among listed methods, approaches such as appearance-based became highly popular because of their resistance to changes in lightning conditions, distance from camera, sensor devices, and orientation. Template-matching methods exhibited great performance on databases with less variability and predicted image elements; they, however, perform poorly on cluttered, obstructed, or low-quality images. Feature-invariant methods or geometric approaches are popular due to their simplicity and fast recognition rates, but presently they are usually augmented with appearance-based methods or template-based methods. Knowledge-based methods were the earliest developed methods and now they are rarely used.

4) *Current Directions:* The first successful attempt to apply a neural-network-based learning system for synthetic fingerprint recognition has been reported in [1]. There are also combined approaches becoming more and more popular with multimodal biometric systems being developed on the basis of a high-dimensional vector representing the

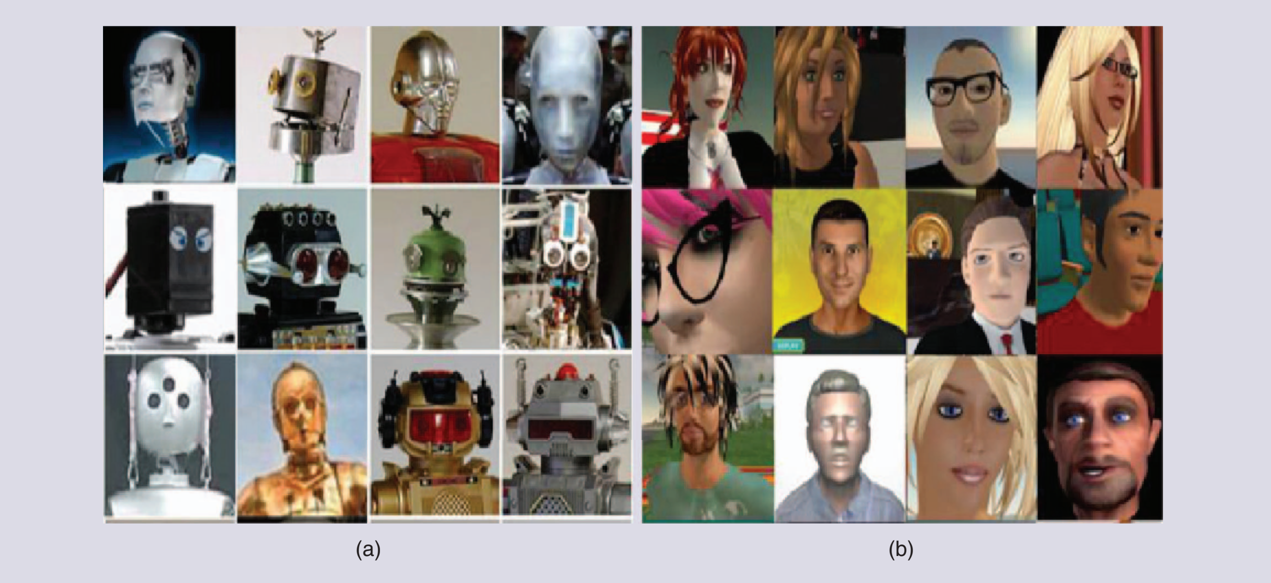


Figure 3. (a) Sample images for a robot face dataset, currently limited to manual collection. (b) Automatically generated random avatar faces [120], [82].

combination of features extracted by variety of the above methods [41]. Recent state-of-the-art research on such complex systems utilizes information fusion for decision making and learning approaches from the AI domain [37].

An important biometric problem is face identification. Holistic methods use the whole face as the input to the recognizer and rely on principal component analysis (PCA) and its variants, such as Eigenfaces [28], Fisherfaces [10], SVM [86], and independent component analysis [8] to perform identification. Feature-based methods work by extracting structural features such as location of the eyes and lips from the image, and that data serve as the input to the classifier, which uses hidden Markov model [96], convolution neural network [65], or graph-matching [116] algorithms to achieve facial pattern identification.

The first results in this area appeared in a 2010 paper [123], coauthored by A. Jain, which introduced concepts of verification and identification of avatar faces. Recent 2011–2012 papers [118], [3], [13], [73], [74] and [130] reported the first numerical results validating approaches on an avatar face database. At the same time, research on behavior artimetrics has commenced.

Behavioral Artimetrics

1) *Goals*: Forensics, and more specifically authorship recognition (sometimes called "stylometry"), is one of the sources of prior research related to behavior-based authentication of identity.
2) *Methods:* In particular, a lot of research has been done in vocabulary analysis and profiling of plain text [52], [62], [63], e-mails [104], [114], and source code [101], [42], [35]. Written text or spoken language, once transcribed, can be analyzed in terms of vocabulary and style to determine its authorship. To do so, a linguistic profile needs to be established. Many linguistic features can be profiled, such as lexical patterns, syntax, semantics, pragmatics, information content, and item distribution through a text [43]. Commonly utilized text descriptors include word count, punctuation mark count, noun phrase count, word included in noun phrase count, prepositional phrase count, word included in prepositional phrase count, and keyword count [102]. Once linguistic features have been established, SVMs [51], Bayesian classifiers [58], multiple regression, and discriminant analysis [103] algorithms (among others) have been applied to determine the authorship of the text.
3) *Current Directions:* At the moment, the CyberSecurity Lab at the University of Louisville is perusing two behavioral artimetrics projects. One project looks at the profiling of vocabulary for Internet chat bots with the goal of identifying a particular bot in new contexts [4]. The second project is aimed at performing voice-based authentication of non-biological speakers such as text-to-speech software, robots, and GPS units.

   Gesture recognition is another area currently being actively researched and is directly applicable to robot behavior authentication. Gestures form an integral part of human communication and are primary candidates for extending the communicative abilities of social robots [95]. In many cases, robot gestures are not produced at run-time, but are prerecorded for specific situations [95]. The latest research aims to produce gestures coupled with the semantic of situations in a dynamic fashion. Consequently, a number of virtual and physical robot systems have been developed, which contain a diverse spectrum of gestures and facial expressions [56], [45], [88]. Artimetrics researchers could record such body language and use it for authentication purposes. Currently no results describing artimetrics systems based on gestures have been reported, but this will soon change as projects are under research in the authors' labs to explore this exciting new area. Below, we present a nonexhaustive list of currently available artificial gesturing systems overviewed by Salem et al. [95] and Kim et al. [56]. As this is a relatively new area of research, we anticipate a lot of developments in this area in the near future and consequently great development in gesture-based artimetrics.
4) *Robot Gestures:* In the world of physical robots, Maggie [41], a personal robot, is one example of a system equipped with a set of predefined gestures, which is also capable of learning gestures from its users. Mel [100], a penguin robot, is capable of demonstrating a set of predefined gestures to indicate engagement behaviors. Fritz [11], a communication robot, uses facial expression, eye-gaze, and gestures to appear livelier while communicating with its users. Its gestures are produced during interaction, and it contains many humanlike arm movements and pointing gestures [95].
5) *Avatar Gestures:* In the domain of virtual robots (avatars), the generation of speech-accompanying gestures is a much more developed area of research [94]. For example, a conversational agent named Rea [19] acts as a real-estate salesperson. Another example is the Behavioral Expression Animation Toolkit (BEAT) [20], which produces synchronized nonverbal behaviors by predicting the timing of gestures from speech by looking at expressive phrases that coincide with the prominent syllables in the speech. Virtual Agent Max [61] represents an integrative architecture, in which the planning of content and form are combined to give meaningful nonverbal utterances [95]. Natural gestures are produced by a kinematic approach that emphasizes the reproduction of humanlike gestures combined with speech [56]. Nakano et al. [75] worked on automatic gesture production for Web-based animated avatars. Applying the above techniques to the behavior authentication of robots on the basis of the way they present themselves, perform their tasks, and communicate is another emerging area of research [4].
6) *Pros and Cons:* Behavioral methods are generally less reliable when it comes to human biometrics, but in the domain of artimetrics, behaviors of bots and human-controlled avatars are more stable compared to easily altered physical characteristics. Although behavioral artimetrics are more challenging to profile due to the large space of possible behaviors, they

present very promising current research essential to establish robot or avatar identity.

Multimodal Artimetrics

Biometric systems based solely on a single biometric may not always identify the entity (human or robot) in the most optimal or precise way. The problem is common for human and robot authentication: some robots might not possess a certain trait that is being recognized; that is, industrial robots might have similar facial features but different voices, gaits, or behavior. Thus, multibiometric system research is emerging as a trend, which helps to overcome the limitations of a single biometric solution [49]. This is especially useful in the presence of complex patterns, conflicting or misleading behavior, abnormal data samples, and intended or accidental mischief. A reliable and successful multibiometric system normally utilizes an effective fusion scheme to combine the information presented by multiple matchers.

Over the last decade, researchers tried different biometric traits with sensor, feature, decision, and match score-level fusion approaches to enhance the security of a biometric system [50], thus enhancing the security and performance of the authentication system. Multimodal biometric approaches improve the overall system accuracy and address issues of nonuniversality, spoofing, noise, and fault tolerance.

Most common approaches in multibiometrics currently rely on multimodal systems, where numerous strategies for decision making are employed. The most successful ones are based on rank-level, decision-level, and match score-level fusion [50]. Other approaches (multisensor, multialgorithm, multiinstance, and multisample) are not as popular due to the overhead associated with either multiple devices, multiple samples stored in the database, or extra time required to run different algorithms. The first article combining face and fingerprint human identification as a true multimodal system was based on match-level fusion introduced by Jain. It is included in the comprehensive review of all multimodal systems [48]. We postulate that in a similar manner, combining behavioral and physical artimetrics in robot authentication or in the virtual worlds can be utilized as part of a physoemotional artimetric system, which is a multimodal system. In addition, another concept of a multidimensional system crossing over between virtual and real worlds can be explored. This multidimensional authentication is the visual authentication of avatar through its creator authentication and vice versa. Research in this domain is emerging, with a number of projects being conducted at BTLab, University of Calgary. Although multimodal system research has become very popular over the past few years, it carries certain challenges. One is the amount of information that needs to be processed such as associated technological and management challenges of obtaining, securely storing, and accessing multiple databases. Another is the increased cost of developing and maintaining such a system and slightly increased processing time, mainly due to the addition of a fusion module. Finally, in the presence of multisource data processing and decision making, certain dimensionality reduction techniques are necessary to ensure real-time system performance.

Applications and Open Problems

There are numerous applications and implications for the methodology of robot and avatar recognition through applying biometric principles to both appearance and behavioral characteristics and utilizing multimodal and multidimensional information fusion.

One outcome is preventing malicious intelligent software from obtaining access to information or system resources and granting it to authorized agents and by doing so, improving the security of virtual communities, social networks, and the country's cyber infrastructure. With exponential growth in the abilities of artificially intelligent agents (bots, software weapons, viruses, and so on) comes the pressing need to secure information and resources from access by unauthorized agents, while at the same time allowing seamless access for the approved software. Behavior-based profiling of software agents provides an unobtrusive way of separating helpful bots from malware. Additional research in artimetrics is expected to produce novel behavior-profiling approaches specifically designed to take advantage of the unique psychology of artificially intelligent programs. Current research on telling humans and robots apart [121], [2], [6], [12], [72] demonstrates this promising direction of research, while there is still a lot of work to be done.

Finding out which agent has performed a given task, in case a number of possible alternatives exist (for demanding responsibility or assigning a reward) in collaborative environments, is another open area of research. Behavioral profiling can be used to uniquely identify a specific type of bot and potentially the bot's owner. Examples of such preliminary work can be found in click fraud and virus detection research. In both domains, unique behavioral signatures can be obtained (sometimes indirectly) from the software agent and can be matched up with known behavioral signatures leading to the attribution of the attack to a particular hacker or a mischievous group.

Securing the interaction between different components of intelligent software or between a human being and an instance of an intelligent software/robot is also an area of high importance for robot security domains. Botnets, groups of intelligent cooperating agent and mixed robot/human teams, are quickly emerging in various applications. Securing their communications is important for further progress in e-commerce, virtual community development, construction, military, and any other industry with heavy reliance on team-based efforts. To communicate securely, identities of all parties wishing to exchange information need to be determined with a high degree of accuracy. Consequently, it is important to develop automatic algorithms, which would give robots the ability to recognize other robots and human beings they are working with. This is another area with a high impact but many unanswered questions, specifically related to numerous alternatives that exist for robot communication (i.e., signals, gestures, voice, and text commands).

Another aspect open for discussion is identity management. Although numerous algorithms exist to authenticate the identity of specific robots/computers on the basis of digital signatures and cryptographic networking protocols, robots have a better chance of fitting in human-dominated environments if they utilize a humanlike approach to identity management, which is advocated in this article. Other applications include detecting cheating in games on the basis of assistance from AI software, providing visual and behavioral search capabilities for virtual worlds, and making it possible for scientists in fields as diverse as biology, communications, and e-business to securely communicate with intelligent assistants and robots. Development of methods presented in this article not only provides a broad base for future solutions in those domains but also opens up new issues related to differences in human and robot behavioral profiling, collaborative environments, features, and unique specifics of virtual environments that need to be taken into account in real-time methodology integration and testing.

Conclusion

This article introduced a new subfield of security research, which transforms and expands the domain of biometrics beyond biological entities to include software and hardware robots, which are rapidly becoming a part of the modern society. Artimetrics research builds on and expands such diverse fields of science as forensics, robotics, stylometry, computer graphics, and security. This article presented a solid motivation for security research in the field of robotics and cyberworlds, including six scenarios for automated matching algorithms followed by the comprehensive survey of robots and methods for robot dataset creation. Description of visual, behavioral, and multimodal artimetrics constituted the core of methodology, with applications and implications of this emerging area further outlined.

The presented research into trustworthy authentication of robots will make society safer and better prepared for the accelerating integration of intelligent technologies into everyday life. Potential benefits come from the applications of the developed algorithms in many diverse areas, for example, recognition of military robots, preventing malicious intelligent software from obtaining access to resources, securing communication between different intelligent agents in virtual communities, determining authorship rights to the results of computation and creative output produced by an AI entity, and identifying semiautonomous software tools used by hackers.

Potential directions for future artimetrics research include the investigation of other visual and behavioral approaches to robot security on the basis of the appearance of new characteristics and abilities in the robots of tomorrow. Even today, it would be possible to expand robotic biometrics beyond faces and vocabulary to intelligent software agents, which mimic higher-order human intelligence. Some examples are provided below, but the list will unquestionably grow as our success with AI technologies progresses and we obtain programs, which are as creative and unique as human beings. We already have programs capable of composing inspiring music [26], drawing beautiful paintings [25], and writing poetry [14], and limits to the known abilities of machines are continuously being extended. It is already technologically feasible to look at profiling text-to-speech software on the basis of voice recognition, translation software on the basis of linguistic signatures, and authentication of game-playing bots on the basis of the strategies employed as demonstrated by the authors [117], [119].

Some other open problems are generation and evaluation of the quality of virtual entity databases and emerging research on face recognition in the virtual world. Such issues as emotion recognition, face recognition in the presence of aging, various geometrical underlying models, different approaches to virtual face representation, and displaying options provide a broad variability of avatar faces. Direct comparison with human face databases and testing the performance of recognition approaches on such databases versus human databases are an exciting unexplored domain of research. Evaluating the degree of variability of avatar databases is another open problem.

It may also be possible in the future to profile different search engines on the basis of the results they produce. Pattern recognition algorithms such as those used for optical character recognition or for biometric recognition can be profiled on the basis of the error rates. Artificial life and computer viruses can be tracked on the basis of their behavioral signatures, and game characters on the basis of a combination of visual and behavioral traits. As hardware robots continue to improve in their humanlike abilities and appearances, potential physical biometrics worthy of examination may include gait, keystroke dynamics, signature, and body part geometry.

Acknowledgment

The authors would like to thank Dr. A.K. Jain for his critical comments in the preparation of the manuscript and Dr. P. Corke for his diligence during the manuscript revision phase. The authors would also like to thank the NSERC for its support in this project.

References

[1] K. Ahmadian and M. Gavrilova, "Transiently chaotic associative network for fingerprint image analysis," *Int. J. Neural Netw. World*, vol. 3, no. 20, pp. 389–403, 2010.

[2] L. V. Ahn, M. Blum, N. Hopper, and J. Langford, *CAPTCHA:* Using Hard AI Problems for Security, *Eurocrypt*. New York: Springer-Verlag, 2003.

[3] S. Ajina, R. V. Yampolskiy, and N. E. B. Amara, "SVM classification of avatar facial recognition," in *Proc. 8th Int. Symp. Neural Networks*, Guilin, China, May/June 2011, pp. 132–142.

[4] N. Ali, M. Hindi, and R. V. Yampolskiy, "Evaluation of authorship attribution software on a chat bot corpus," in *Proc. 23rd Int. Symp. Information, Communication Automation Technologies, Sarajevo*, Bosnia, Oct. 2011, pp. 1–6.

[5] H. Asoh, S. Hayamizu, I. Hara, Y. Motomura, S. Akaho, and T. Matsui, "Socially embedded learning of the office-conversant mobile robot jijo-2," in *Proc. 15th Int. Joint Conf. Artificial Intelligence*, 1997, pp. 880–885.

[6] H. S. Baird and J. L. Bentley, "Implicit CAPTCHAs," in *Proc. SPIE/IS&T Conf. Document Recognition Retrieval XII*, San Jose, CA, Jan. 2005, pp. 191–196.

[7] D. Barrios-Aranibar and P. J. Alsina, "Recognizing behaviors patterns in a micro robot soccer game," in *Proc. 5th Int. Conf. Hybrid Intelligent Systems*, Washington, DC, Dec. 2005, pp. 463–468.

[8] M. S. Bartlett, H. M. Lades, and T. Sejnowski, "Independent component representation for face recognition," in *Proc. SPIE Symp. Electronic Imaging: Science Technology*, 1998, pp. 528–539.

[9] Second Life 'Child Abuse' Claim, BBC News, (2007, May 9) [Online]. Available: http://news.bbc.co.uk/2/hi/technology/6638331.stm

[10] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs fisherfaces," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 19, no. 7, pp. 711–720, 1997.

[11] M. Bennewitz, F. Faber, D. Joho, and S. Behnke, "Fritz—a humanoid communication robot," in *Proc. 16th IEEE Int. Symp. Robot Human Interactive Communication*, 2007, pp. 1072–1077.

[12] J. Bentley and C. L. Mallows, "CAPTCHA challenge strings: Problems and improvements," *Avaya Labs*, Basking Ridge, NJ, Tech. Rep., Jan. 2006, pp. 141–147.

[13] M. Bouhhris, M. Beck, A. Mahamed, N. E. B. Amara, D. D'Souza, R. V. Yampolskiy, "Artificial human-face recognition via Daubechies wavelet transform and SVM," in *Proc. 16th Int. Conf. Computer Games*, Louisville, KY, July 2011, pp. 18–25.

[14] J. Boyd-Graber. (2006). Semantic Poetry Creation Using Lexicographic and Natural Language Texts [Online]. Available: cs.princeton.edu/~jbg/documents/poetry.pdf

[15] R. S. Boyd. (2010, Apr. 10). Feds Thinking Outside the Box to Plug Intelligence Gaps [Online]. Available: http://www.mcclatchydc.com/2010/03/29/91280/fedsthinking-outside-the-box.html

[16] C. Breazeal, "Sociable machines: Expressive social exchange between humans and robots," *Ph.D. thesis, Dept. Electr. Eng. Comput. Sci., Massachusetts Inst. Technol.*, Cambridge, 2000.

[17] A. Bruce, I. Nourbakhsh, and R. Simmons, "The role of expressiveness and attention in human-robot interaction," in *Proc. AAAI Fall Symp. Emotional Intelligent II*, 2001, pp. 4138–4142.

[18] L. Canamero and J. Fredslund, "I show you how i like you—can you read it in my face?" *IEEE Trans. Syst., Man Cybern. A: Syst. Humans*, vol. 31, no. 5, pp. 454–459, Sept. 2001.

[19] J. Cassell, T. Bickmore, L. Campbell, H. Vilhjalmsson, and H. Yan, "Human conversation as a system framework: Desigining embodied conversational agents," in *Embodied Conversational Agents*. Cambridge, MA: MIT Press, 2000, pp. 29–63.

[20] J. Cassell, H. Vilhjalmsson, and T. Bickmore, "Beat: The behavior expression animation toolkit," in *Proc. SIGGRAPH'01*, 2001, pp. 477–486.

[21] T. Chaminade, M. Zecca, S. Blakemore, A. Takanishi, C. Frith, S. Micera, P. Dario, G. Rizzolatti, V. Gallese, and M. Umilta, "Brain response to a humanoid robot in areas implicated in the perception of human emotional gestures," *PLoS ONE*, vol. 5, no. 7, p. e11577, 2010.

[22] J. S. Charles, C. Rosenberg, and S. Thrun, "Spontaneous, short-term interaction with mobile robots," in *Proc. IEEE Int. Conf. Robotics Automation*, 1999, pp. 658–663.

[23] J. S. Charles, C. Rosenberg, and S. Thrun, "Spontaneous, short-term interaction with mobile robots in public places," in *Proc. IEEE Int. Conf. Robots Automation*, May 1999, pp. 658–663.

[24] K.-J. Chen and J.-P. Barthes, "Giving an office assistant agent a memory mechanism," in *Proc. 7th IEEE Int. Conf. Cognitive Informatics*, Compiegne, France, 2008, pp. 402–410.

[25] H. Cohen. (1998). How To Draw Three People in a Botanical Garden [Online]. Available: crca.ucsd.edu/~hcohen/cohenpdf/how2draw3people.pdf

[26] D. Cope, Virtual Music: Computer Synthesis of Musical Style. Cambridge, MA: MIT Press, 2001, p. 579.

[27] M. Corney, O. D. Vel, A. Anderson, and G. Mohay, "Gender-preferential text mining of e-mail discourse," in *Proc. 18th Annu. Computer Security Applications Conf.*, Brisbane, Australia, 2002, pp. 282–289.

[28] I. Craw and P. Cameron, "Face recognition by computer," in *Proc. British Machine Vision Conf.*, 1996, pp. 489–507.

[29] I. Craw, D. Tock, and A. Bennett, "Finding face features," in *Proc. 2nd European Conf. Computer Vision, Santa Margherita Ligure*, Italy, 1992, pp. 92–96.

[30] Y. Dai and Y. Nakano, "Face-texture model based on SGLD and its application in face detection in a color scene," *Pattern Recognit.*, vol. 29, no. 6, pp. 1007–1017, 1996.

[31] F. Delaunay, J. D. Greeff, and T. Belpaeme, "A study of a retro-projected robotic face and its effectiveness for gaze reading by humans," *in Proc. 5th ACM/IEEE Int. Conf. Human-Robot Interaction*, Osaka, Japan, 2010, pp. 39–44.

[32] C. Elliot and W. L. Johnson, "I picked up Catapia and other stories: A multimodal approach to expressivity for emotionally intelligent agents," in *Proc. Int. Conf. Autonomous Agents*, 1997, pp. 451–457.

[33] E. Feldmann. (2008, Oct. 23). Netherlands teen sentenced for stealing virtual goods, *PC World* [Online]. Available: www.pcworld.com/businesscenter/article/152673/

[34] T. W. Fong, I. Nourbakhsh, and K. Dautenhahn, "A survey of socially interactive robots," *Robot. Auton. Syst.*, vol. 42, nos. 3–4, pp. 143–166, 2003.

[35] G. Frantzeskou, S. Gritzalis, and S. Macdonell, "Source code authorship analysis for supporting the cybercrime investigation process," *in Proc. 1st Int. Conf. eBusiness Telecommunication Networks*, Setubal, Portugal, Aug. 2004, pp. 85–92.

[36] W. Gao, B. Cao, S. Shan, X. Chen, D. Zhou, X. Zhang, and D. Zhao, "The CAS-PEAL large-scale Chinese face database and baseline evaluations," *IEEE Trans. Syst., Man Cybern., A*, vol. 38, no. 1, pp. 149–161, 2008.

[37] M. Gavrilova and M. Monwar, "Pattern recognition and biometric fusion," in *Pattern Recognition, Machine Intelligence Biometric, P. Wang, Ed.* New York: Springer-Verlag, 2011.

[38] M. Gavrilova and R. Yampolskiy, "Applying biometric principles to avatar recognition," *Trans. Comput. Sci. XII*, vol. 6670, pp. 140–158, 2011.

[39] S. Gianvecchio, M. Xie, Z. Wu, and H. Wang, "Measurement and classification of humans and bots in internet chat," *in Proc. 17th Conf. Security Symp.*, San Jose, CA, 2008, pp. 155–169.

[40] K. M. Godby and J. A. Lane, "Robot self-recognition using conditional probability-based contingency," *in Proc. 21st Nat. Conf. Artificial Intelligence*, Boston, MA, 2006, pp. 1869–1870.

[41] J. F. Gorostiza, R. Barber, A. M. Khamis, M. Malfaz, R. Pacheco, R. Rivas, A. Corrales, E. Delgado, and M. A. Salichs, "Multimodal human-robot interaction framework for a personal robot," in *Proc. 15th IEEE Int. Symp. Robot Human Interactive Communication*, 2006, pp. 1–6.

[42] A. Gray, P. Sallis, and S. Macdonell, "Software forensics: Extending authorship analysis techniques to computer programs," in *Proc. 3rd Biannual Conf. Int. Association Forensic Linguists*, 1997, pp. 1–10.

[43] H. V. Halteren, "Linguistic profiling for author recognition and verification," in *Proc.42nd Annu. Meeting Association Computational Linguistics*, 2004. pp. 1–7.

[44] K. Han and M. Veloso, "Automated robot behavior recognition," in *Proc. Workshop Team Behaviors Plan Recognition*, 1999, pp. 1–8.

[45] Y. Hattori, H. Kozima, K. Komathi, T. Ogata, and H. G. Okuno, "Robot gesture generation from environmental sounds using inter-modality mapping," in *Proc. 5th Int. Workshop Epigenetic Robotics*, Nara, Japan, 2006, pp. 139–140.

[46] Honda. (2010, June 1). *Honda Worldwide, Asimo – History* [Online]. Available: http://world.honda.com/ASIMO/history

[47] J. Ito. (2009, Mar. 16). *Fashion Robot to Hit Japan Catwalk* [Online]. Available: www.physorg.com/pdf156406932.pdf

[48] A. Jain and S. Z. Li, *Handbook on Face Recognition*. New York: Springer-Verlag, July 2004.

[49] A. K. Jain, S. C. Dass, and K. Nandakumar, "Soft biometric traits for personal recognition systems," in *Proc. Int. Conf. Biometric Authentication*, Hong Kong, July 2004, pp. 731–738.

[50] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forens. Security*, vol. 1, no. 2, pp. 125–143, 2006.

[51] D. Joachim, K. Jorg, L. Edda, and G. Paass, "Authorship attribution with support vector machines," *Appl. Intell.,* vol. 19, nos. 1–2, pp. 19–123, 2003.

[52] P. Juola and J. Sofko, "Proving and improving authorship attribution," in *Proc. Canadian Symp. Text Analysis*, 2006, pp. 1–8.

[53] K. Karimi, M. Mehrandezh, and H. J. Hamilton, "A proposal for self-recognition in robot programming," in *Proc. Canadian Conf. Electrical Computer Engineering*, May 2005, pp. 657–660.

[54] U. Kaufmann, G. Mayer, G. Kraetzschmar, and G. Palm, *Visual Robot Detection in Robocup Using Neural Networks* (Lecture Notes Computer Science). New York: Springer-Verlag, 2005, pp. 262–273.

[55] J. Khurshid and H. Bing-Rong, "Military robots—a glimpse from today and tomorrow," in *Proc. 8th Control, Automation, Robotics Vision Conf.*, 2004, pp. 771–777.

[56] H.-H. Kim, H.-E. Lee, Y.-H. Kim, K.-H. Park, and Z. Z. Bien, "Automatic generation of conversational robot gestures for human-friendly Steward robot," in *Proc. 16th IEEE Int. Symp. Robot Human Interactive Communication*, Aug. 2007, pp. 1155–1160.

[57] D. Kirsch, "The affective Tigger: A study on the construction of anemotionally reactive toy," *M.S. thesis. Progr. Media Arts Sci., Massachusetts Institute of Technology*, Cambridge, 1999.

[58] B. Kjell, "Authorship attribution of text samples using neural networks and Bayesian classifiers," in *Proc. IEEE Int. Conf. Systems, Man, Cybernetics*, San Antonio, TX, 1994, pp. 1660–1664.

[59] B. Klimpak, M. Grgic, and K. Delac, "Acquisition of a face database for video surveillance research," in *Proc. 48th Int. Symp. Focused Multimedia Signal Communications*, Zadar, Croatia, 2006, pp. 111–114.

[60] H. Kobayashi and F. Hara, "Study on face robot for active human interface-mechanisms of facerobot and expression of 6 basic facial expressions," in *Proc. 2nd IEEE Int. Workshop Robot Human Communication*, Tokyo, Japan, Nov 1993, pp. 276–281.

[61] S. Kopp and I. Wachsmuth, "Synthesizing multimodal utterances for conversational agents," *Comput. Animat. Virtual Worlds*, vol. 15, no. 1, pp. 39–52, 2004.

[62] M. Koppel and J. Schler, "Authorship verification as a one-class classification problem," in *Proc. 21st Int. Conf. Mach. Learn.*, Banff, AB, Canada, July 2004, pp. 489–495.

[63] M. Koppel, J. Schler, and D. Mughaz, "Text categorization for authorship verification," in *Proc. 8th Int. Symp. Artificial Intelligence Mathematics*, Fort Lauderdale, FL, Jan. 2004, pp. 1–11.

[64] A. Lanitis, C. J. Taylor, and T. F. Cootes, "An automatic face identification system using flexible appearance models," *Image Vis. Comput.*, vol. 13, no. 5, pp. 393–401, 1995.

[65] S. Lawrence, C. L. Giles, A. C. Tsoi, and A. D. Back, "Face recognition: A convolutional neural-network approach," *IEEE Trans. Neural Netw.*, vol. 8, no. 1, pp. 98–113, 1997.

[66] S. Li and A. Jain, Eds. *Handbook of Face Recognition-Face Databases*. New York: Springer-Verlag, 2005.

[67] H.-O. Lim and A. Takanishi, "Waseda biped humanoid robots realizing humanlike motion," in *Proc. 6th Int. Workshop Advanced Motion Control*, Nagoya, Japan, 2000, pp. 525–530.

[68] R. Lynn. Virtual Rape is Traumatic, But is it a Crime? Wired. (2007, May 4) [Online]. Available: www.wired.com/culture/lifestyle/commentary/sexdrive/2007/05/sexdrive_0504

[69] M. Lyons, A. Plante, S. Jehan, S. Inoue, and S. Akamatsu, "Avatar creation using automatic face recognition," in *Proc. ACM Multimedia 98*, Bristol, England, pp. 427–434.

[70] S. Mckenna, S. Gong, and Y. Raja, "Modelling facial colour and identity with Gaussian mixtures," *Pattern Recognit.*, vol. 31, no. 12, pp. 1883–1892, 1998.

[71] P. Miller. (2010, June 1). Hiroshi Ishiguro Builds his Evil Android Twin: Geminoid HI-1 [Online]. Available at: http://www.engadget.com/2006/07/21/hiroshi-ishigurobuilds-his-evil-android-twin-geminoid-hi-1

[72] D. Misra and K. Gaj, "Face recognition CAPTCHAs," in *Proc. Int. Conf. Telecommunications, Internet Web Applications Services*, Feb. 2006, p. 122.

[73] A. Mohamed, N. Baili, D. D'souza, and R. V. Yampolskiy, "Avatar face recognition using wavelet transform and hierarchical multi-scale LBP," in *Proc. 10th Int. Conf. Machine Learning Applications*, Honolulu, HI, Dec. 2011, pp. 194–199.

[74] A. Mohamed and R. V. Yampolskiy, "An improved LBP algorithm for Avatar face recognition," in *Proc. 23rd Int. Symp. Information, Communication Automation Technologies*, Sarajevo, Bosnia, Oct. pp. 1–5.

[75] Y. I. Nakano, M. Okamoto, and T. Nishida, *Enriching Agent Animations with Gestures and Highlighting Effects* (Lecture Notes Computer Science), vol. 3490. New York: Springer-Verlag, 2005, pp. 91–98.

[76] S. Nof, Ed., *Handbook of Industrial Robotics*. New York: Wiley, 1999.

[77] N. Nosengo, "Robotics: The bot that plays ball," *Nature*, vol. 460, no. 7259, pp. 1054–1078, 2009.

[78] N. O'brien. (2007, July 31). Spies Watch Rise of Virtual Terrorists [Online]. Available at: http://www.news.com.au/spies-watch-rise-of-virtualterrorists/story-e6frfkp9-1111114075761

[79] R. O'harrow. (2008, Feb. 6). Spies' Battleground Turns Virtual [Online]. Available at: www.washingtonpost.com/wp-dyn/content/article/2008/02/05/AR2008020503144.html

[80] J.-H. Oh, D. Hanson, W.-S. Kim, I. Y. Han, Y. Han, and I.-W. Park, in *Proc. Int. Conf. Intelligent Robots Systems*, Daejeon, Korea, 2006, pp. 1428–1433.

[81] E. Osuna, R. Freund, and F. Girosi, "training support vector machines: An application to face detection," in *Proc. IEEE Conf. Computer Vision Pattern Recognition*, 1997, pp. 130–136.

[82] J. N. Oursler, M. Price, and R. V. Yampolskiy, "Parameterized generation of Avatar face dataset," in *Proc. 14th Int. Conf. Computer Games*. Louisville, KY, 2009, pp. 1–6.

[83] D. Ourston, "Program recognition," *IEEE Expert*, vol. 4, no. 4, pp. 36–49, 1989.

[84] A. Pasick. (2007, Apr. 4). *FBI Checks Gambling in Second Life Virtual World* [Online]. Available at: www.reuters.com/article/idUSHUN43981820070405

[85] P. Patel and H. Hexmoor, "Designing BOTs with BDI agents," in *Proc. Int. Symp. Collaborative Technologies Systems*, Carbondale, IL, 2009, pp. 180–186.

[86] P. J. Phillips, "Support vector machines applied to face recognition," *in Proc. Advances Neural Information Processing Systems,* vol. 11, pp. 803–809, Mar. 1998.

[87] A. Quilici, Q. Yang, and S. Woods, "Applying plan recognition algorithms to program understanding," *Autom. Softw. Eng.: Int. J.*, pp. 347–372, July 1998.

[88] L. Rai, B.-H. Lee, J. Hong, and H. Hahn, "Intelligent gesture generation in humanoid robot using multi-component synchronization and coordination, in Proc. ICROS-SICE Int. Joint Conf., Fukuoka, Japan, Aug. 2009, pp. 1388–1392.

[89] A. Rajagopalan, K. Kumar, J. Karlekar, R. Manivasakan, M. Patil, U. Desai, P. Poonacha, and S. Chaudhuri, "Finding faces in photographs," *in Proc. IEEE Int. Conf. Computer Vision*, 1998, pp. 640–645.

[90] L. D. Riek, T.-C. Rabinowitch, P. Bremner, A. G. Pipe, M. Fraser, and P. Robinson, "Cooperative gestures: Effective signaling for humanoid robots," *in Proc. 5th ACM/IEEE Int. Conf. Human-Robot Interaction*, Osaka, Japan, 2010, pp. 61–68.

[91] H. Rowley, S. Baluja, and T. Kanade, "Neural network-based face detection, *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, no. 1, pp. 23–38, 1998.

[92] M. Saerbeck and C. Bartneck, "Perception of affect elicited by robot motion," *in Proc. 5th ACM/IEEE Int. Conf. Human-Robot Interaction*, Osaka, Japan, 2010, pp. 53–60.

[93] H. Sahin and L. Guvenc, "Household robotics: Autonomous devices for vacuuming and lawn mowing," *IEEE Control Syst. Mag.*, vol. 27, no. 2, pp. 20–96, 2007.

[94] M. Salem, S. Kopp, I. Wachsmuth, and F. Joublin, "Generating robot gesture using a virtual agent framework," *in Proc. IEEE/RSJ Int. Conf. Intelligent Robots Systems*, Taipei, Taiwan, Oct. 2010 pp. 3592–3597.

[95] M. Salem, S. Kopp, I. Wachsmuth, and F. Joublin, "Towards meaningful robot gesture," *Cognit. Syst. Monogr.*, vol. 6, pp. 173–182, Jan. 2009.

[96] F. Samaria and S. Young, "HMM based architecture for face identification," *Image Vis. Comput.*, vol. 12, no. 8, pp. 537–583, 1994.

[97] R. G. Satter. (2009, Dec.). *Facebook Fugitive Taunts British Police [Online].* Available: http://www.msnbc.msn.com/id/34625567/

[98] M. Scheeff, "Experience with sparky: A social robot," *in Proc. Workshop Interactive Robot Entertainment, Pittsburgh*, PA, 2000, pp. 1–8.

[99] H. Schneiderman and T. Kanade, "Probabilistic modeling of local appearance and spatial relationships for object recognition," *in Proc. IEEE Computer Vision Pattern Recognition*, 1998, pp. 45–51.

[100] C. L. Sidner, C. Lee, and N. Lesh, "The role of dialog in human robot interaction," *in Proc. Int. Workshop Language Understanding Agents Real World Interaction*, 2003, pp. 1–7.

[101] E. H. Spafford and S. A. Weeber, "Software forensics: Can we track code to its authors?" *in Proc. 15th Nat. Computer Security Conf.*, Oct. 1992, pp. 641–650.

[102] E. Stamatatos, N. Fakotakis, and G. Kokkinakis, "Automatic authorship attribution," *in Proc. 9th Conf. European Chapter Association Computational Linguistics,* Bergen, Norway, June 1999, pp. 158–164.

[103] E. Stamatatos, N. Fakotakis, and G. Kokkinakis, "Computer-based authorship attribution without lexical measures," *Comput. Human.*, vol. 35, no. 2, pp. 193–214, 2001.

[104] S. J. Stolfo, S. Hershkop, K. Wang, O. Nimeskern, and C.-W. Hu, "A behavior-based approach to securing email systems," *Math. Methods, Models Arch. Comput. Netw. Security*, vol. 2776, pp. 57–81, Jan. 2003.

[105] K. Sullivan. (2008, Apr. 3). Virtual Money Laundering and Fraud—Second Life and Other Online Sites Targeted by Criminals. [Online]. Available: www.bankinfosecurity.com/articles.php?art_id=809

[106] D. Talbot. (2008, Jan.). *The Fleecing of the Avatars* [Online]. Available: www.technologyreview.com/Infotech/19844/

[107] X. Tan, S. Chen, Z.-H. Zhou, and F. Zhang, "Face recognition from a single image per person: A survey," *Pattern Recognit.*, vol. 39, no. 9, pp. 1725–1745, 2006.

[108] K. Tanaka and Y. Kimuro, "Motion sequence scheme for detecting mobile robots in an office environment," *in Proc. IEEE Int. Symp. Computational Intelligence Robotics Automation*, 2003, pp. 145–150.

[109] H. Tang, Y. Fu, J. Tu, M. Hasegawa-Johnson, and T. S. Huang, "Humanoid audio–visual avatar with emotive text-to-speech synthesis," *IEEE Trans. Multimedia*, vol. 10, no. 6, pp. 969–981, 2008.

[110] D. Teijido, "Information assurance in a virtual world," *in Proc. Australasian Telecommunications Networks Applications Conf.*, Canberra, Australia, Nov. 2009.

[111] A. Toor. (2010, June 25). *AWOL Afghan Soldiers Actively Used Facebook*, Even While at Large [Online]. Available: http://www.switched.com/2010/06/25/awol-afghan-soldiers-activelyused-facebook-even-while-at-large/

[112] M. Turk and A. Pentland, "Eigenfaces for recognition," *J. Cognit. Neurosci.*, vol. 3, no. 1, pp. 71–86, 1991.

[113] A. Turner. (2007). *Second Life Charges for Real Names, Increases Identity Theft Risk [Online].* Available at: http://www.itwire.com/opinion-andanalysis/seeking-nerdvana/11110-second-life-charges-for-real-namesincreases-identity-theft-risk

[114] O. D. Vel, A. Anderson, M. Corney, and G. Mohay, "Mining email content for author identification forensics," *ACM SIGMOD Rec.: Special Sect. Data Mining Intrus. Detect. Threat Anal.*, vol. 30, no. 4, pp. 55–64, 2001.

[115] M. Wagner. (2007, May 26). *Sex in Second Life, Information Week [Online].* Available: http://www.informationweek.com/news/software/hosted/showArticle.jhtml?articleID=199701944

[116] L. Wiskott, J.-M. Fellous, and C. V. D. Malsburg, "Face recognition by elastic bunch graph matching," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 19, no. 7, pp. 775–779, 1997.

[117] R. V. Yampolskiy, "Behavioral biometrics for verification and recognition of AI programs," *in Proc. 20th Annu. Computer Science Engineering Graduate Conf., Buffalo, NY*, 2007, pp. 1–11.

[118] R. V. Yampolskiy, G. Cho, R. Rosenthal, and M. L. Gavrilova, "Evaluation of face detection and recognition algorithms on Avatar face datasets," *in Proc. Int. Conf. Cyberworlds, Banff, AB*, Canada, Oct. 2011, pp. 93–99.

[119] R. V. Yampolskiy and V. Govindaraju, "Behavioral biometrics for recognition and verification of game bots," *in Proc. 8th Annu. European Game-On Conf.*, Bologna, Italy, Nov. 2007, pp. 108–114.

[120] R. V. Yampolskiy and V. Govindaraju, "Behavioral biometrics for verification and recognition of malicious software agents," *in Proc. SPIE Defense Security Symp.*, Orlando, FL, Mar. 2008, pp. 1–11.

[121] R. V. Yampolskiy and V. Govindaraju, "Embedded non-interactive continuous bot detection," *ACM Comput. Entertain.*, vol. 5, no. 4, pp. 1–11, 2007.

[122] R. V. Yampolskiy and V. Govindaraju, "Strategy-based behavioral biometric a novel approach to automated identification," *Int. J. Comput. Appl. Technol.*, vol. 35, no. 1, pp. 29–41, 2009.

[123] R. V. Yampolskiy, B. Klare, A. K. Jain, "Face recognition in the virtual world: Recognizing Avatar faces," in *Proc. 11th Int. Conf. Machine Learning Applications*, Boca Raton, FL, Dec. 2012, pp. 1–7.

[124] G. Yang and T. S. Huang, "Human face detection in complex background," *Pattern Recognit.*, vol. 27, no. 1, pp. 53–63, 1994.

[125] M.-H. Yang, D. J. Kriegman, and N. Ahuja, "Detecting faces in images: A survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 1, pp. 34–58, 2002.

[126] S. Yanushkevich, M. Gavrilova, P. Wang, and S. Srihari, *Image Pattern Recognition: Synthesis and Analysis in Biometrics.* Singapore: World Scientific, 2007.

[127] S. N. Yanushkevich, S. Stoica, and V. P. Shmerko, "Synthetic biometrics," *Comput. Intell. Mag.*, vol. 2, no. 2, pp. 60–69, 2007.

[128] K. C. Yow and R. Cipolla, "Feature-based human face detection," Image Vis. Comput., vol. 15, no. 9, pp. 713–735, 1997.

[129] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," *ACM Comput. Surveys*, vol. 35, no. 4, pp. 399–458, 1997.

[130] A. Mohamed, M. Gavrilova, and R. Yampolskiy "Artificial face recognition using wavelet adaptive LBP with directional statistical features," in *Proc. CyberWorlds IEEECS 2012.*

Roman V. Yampolskiy, Department of Computer Engineering and Computer Science, Speed School of Engineering. University of Louisville. Louisville, Kentucky, USA. E-mail: roman.yampolskiy@louisville.edu.

Marina L. Gavrilova, University of Calgary, Calgary, AB, Canada. E-mail: marina@cpsc.ucalgary.ca.