Applying Biometric Principles to Avatar Recognition

Marina L. Gavrilova[1] and Roman Yampolskiy[2]

[1] Dept. of Computer Science, University of Calgary, Canada
marina@cpsc.ucalgary.ca
[2] Dept. of Computer Engineering and Computer Science, University of Louisville, USA
roman.yampolskiy@louisville.edu

Abstract. Domestic and industrial robots, intelligent software agents, and virtual world avatars are quickly becoming a part of our society. Just like it is necessary to be able to accurately authenticate identity of human beings, it is becoming essential to be able to determine identities of the non-biological entities. This paper presents current state of the art in virtual reality security, focusing specifically on emerging methodologies for avatar authentication. It also makes a strong link between avatar recognition and current biometric research. Finally, future directions and potential applications for this high impact research field are discussed.

Keywords: biometric, avatar, recognition, robot, synthesis, artimetrics.

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.

In Alan Turings's 1950 work "Computing Machinery and Intelligence," Turing posed the question "can machines think?" In order to establish a credible criteria to answer this question, he proposed a test, now widely known as "The Turing Test" – to estimate 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 behavioural biometric, which can detect differences between a man and the machine. After the theoretical platform for an Automated Turing Test (ATT) was developed by Naor in 1996, the new generation of researchers continued to study the same concept of human / machine disambiguation. In addition to ATT, the new developed procedures were "reversed Turing test" (RTT); "human interactive proof" (HIP); "mandatory human participation" (MHP); and the "completely automated public Turing test to tell computers and humans apart" (CAPTCHA) [1].

M.L. Gavrilova et al. (Eds.): Trans. on Comput. Sci. XII, LNCS 6670, pp. 140–158, 2011.

Following Turing's work, another foundation of modern artificial intelligence was laid out by John von Neumann in the 1950's in his theory of automata and self-replicating machines. His theoretical concepts were based on those of Alan Turing. The main difference was that instead of being able to read and write data, a self-replicating system reads instructions and converts these into assembly commands that result in the assembly of replicas of the original machine. The vast majority of work in this area is in the form of non-physical self-replicating automata (e.g., computer viruses, the "game of life" computer program, etc.). The only physically based concepts that have been explored related to true self-replication pertain to self-assembling systems and robots.

Self-replication is an essential feature in the definition of living things. At the core of biological self-replication lies the fact that nucleic acids can produce copies of themselves when the required chemical building blocks and catalysts are present. This self-replication at the molecular level gives rise to reproduction in the natural world on length scales ranging the ten orders of magnitude. Self-replication in non-biological contexts has been investigated as well, but to a much lesser degree. These efforts have resulted in the field of "Artificial Life". This field is concerned with the sets of rules that, when in place, lead to patterns that self-replicate. The research has been fruitful in the past decade. Cornell University researchers have created a machine that can build copies of itself. Their robots are made up of a series of modular cubes -- called "molecubes" -- each containing identical machinery and the complete computer program for replication. The cubes have electromagnets on their faces that allow them to selectively attach to and detach from one another, and a complete robot consists of several cubes linked together.

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 plentiful. 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 becoming essential to be able to determine identity of the non-biological entities rapidly infiltrating all aspects of modern society. Military soldier-robots [27], robots museum guides [6], software office assistants [7], human-like biped robots [35], office robots [2], bots [44], robots with human-like faces [31], virtual world avatars [57] 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, we proposed [62, 65, 64] the concept of *Artimetrics* – a field of study that will allow identifying, classifying and authenticating robots, software and virtual reality agents. In this paper, unless otherwise qualified, the word *robot (or agent)* refers to all of the above mentioned non-biological entities.

While the area of robot and agent authentication may seem a bit futuristic at first, careful analysis of recent news stories shows that the proposed research is years behind where it needs to be.

Fig. 1. Facial images of a humanoid robot-model, robot celebrity and a 3D-virtual avatar [41] [22] [43]

To give just some examples: Al-Qaeda terrorists have been reported recruiting and communicating in virtual communities such as Second Life [8]. Cybercrime, including identity theft, is rampant in virtual worlds populated by millions of avatars and operating multibillion dollar economies [40]. Security experts have testified to the US Senate that defenses are lacking when it comes to emerging threats to the nation's Cyberinfrastructure. International teams of hackers assisted by semiautomatic hacking software agents have perpetrated numerous attacks against the Pentagon and other government agencies' computers and networks [59].

A novel paradigm, unique to virtual communities, has appeared in recent years and was labeled "interreality''. In the *Second Life* visitors are allowed to populate, build and exploit initially empty spaces. As a result "the new reality that is thus created is, remarkably enough not entirely 'virtual', but is becoming gradually more linked to our physical reality" [40]. Relationships between social, economical, and psychological status of game players and their respected avatars in the virtual environment are a subject of current research. Early results show that avatars for the most parts resemble their "owners" rather than being completely virtual creations. As the physical and the virtual worlds seem to come really close to each other, the distinction between the two begins to fade and the need arises for security systems capable of working in the contexts of interreality and augmented reality [37]. In his dissertation 'Architecture of a Cyber Culture' published in 2003, Van Kokswijk describes this phenomenon as "the hybrid and absolute experience of physical and virtual reality". Interreality is the creation of a hybrid total image of and in both the physical and virtual worlds. Unfortunately, currently available biometric systems are not designed to handle visual and behavioral variations observed in non-human agents and consequently perform extremely poorly if applied outside of their native domain.

The question of security and identification of avatars in this "interreality" consistently arises. Based on research and polls performed on Internet forums, people often complain about the insufficient security in Second Life, with almost 40% of the respondents asking for additional security [40]. More than half of the respondents admit they have been harassed (this includes imprisoning, stalking, gossiping and using inappropriate language) and 40% indicate that certain actions should not be permitted in Second Life. Thus, the definite need in increasing and enforcing security is apparent, which motivates emerging research on security in the increasingly complex and interrelated virtual worlds.

It is interesting to note that some biometric methods came very close to avatar development and intelligent robots/software authentication on a number of different

instances. For example, in 1998 M.J. Lyons and his colleagues published a report: "*Avatar Creation using Automatic Face Recognition",* where authors discuss specific steps and processing techniques that need to be taken in order for avatar to be created almost automatically from the human face [36]. In fact, the process described in the above article is essentially the process of biometric synthesis, conceptualized and generalized in the book devoted specifically to this subject [69]. Users of virtual words have also noted that avatars very often resemble the characteristics of its creator, and not only facial characteristics, but also body shape, accessories and clothes.

But what about other less obvious resemblances such as manner of communication, various situation response, nature of work, style of house, leisure/recreational activities, time of appearing in virtual world etc.? All of the above encompasses behavioral characteristics that can be exploited by the fusion of biometric-based techniques, with methodology tailored to specifics of virtual world. Such behavioral characteristics, as authors of this article would postulate, 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 creation of a consistent virtual image but would not so easily change their patterns of behavior.

The rest of this paper is organized as follows: a literature review is presented in Section 2, a comprehensive survey of non-biological entities (avatars) is given in Section 3, an overview of methodology under development, focusing on dataset creation, synthetic biometrics, visual, behavioral and multi-modal artimetrics constitutes Section 4, applications and implications of this emerging area are outlines in Section 5 and finally concluding summary is provided in Section 6.

2 Literature Review

To the best of our knowledge, no paper surveying automatic visual or behavioral authentication of software agents, virtual reality entities or hardware robots has been published to date. While no research has been reported in automatic robot authentication or behavior analysis some relevant research has been published on robot emotion recognition [13]. In addition to experiments on understanding of emotional states of robots, some work has been started on general analysis of *avatar behavior*. One of the projects is developed under the heading Avatar DNA. Together the segments define the makeup of an avatar. The genes of the avatar are unique and include user biometric data, public key information, personal information, authentication information, creation data, etc. Verification modules in the virtual world collect information directly from the avatar to establish the roles and rights that should be granted to this user [58].

In another experiment linking real world and the world of avatars, William Steptoe asked eleven volunteers some personal questions. During the interviews the volunteers wore eye-tracking devices. A second group of volunteers watched videos of avatars as they delivered first group's answers. Some avatars had eye movements that mirrored those of the original volunteers, while others did not. The volunteers had to determine if the avatar was lying to them. Eye-movement allowed increasing accurate detection of truthful statements from 70% to 88% and detection of lies from 39% to

48% clearly demonstrating importance of even subtle body language in virtual world communication and avatar behavioral analysis [12].

Multiplayer online computer games are quickly growing in popularity, with millions of players logging in every day. While most play in accordance with the rules set up by the game designers, some choose to utilize artificially intelligent assistant programs, a.k.a. bots, to gain an unfair advantage over other players. A recently published paper by one of the authors of this work demonstrated feasibility of applying strategy-based purely behavioral biometrics developed for recognition of human beings to the recognition of intelligent software agents [65]. The paper lays the theoretical groundwork for the research in authentication of non-biological entities. The possibility that behavior-based biometric systems can be spoofed in particular by artificially intelligent software agents [63] was also addressed, which lead to research on automatically telling bots and humans apart [66]. Authors of the paper demonstrate how an embedded non-interactive test can be used to prevent automatic artificially intelligent players from illegally participating in online game-play. Specifically, they demonstrated that behavioral biometrics is a great approach to intelligent software authentication.

3 Survey of Non-biological Entities

There are three main types of non-biological entities, that can be broadly classified as Virtual Beings (avatars), Intelligent Software Agents (bots), and Hardware Robots [21]. Virtual Being are at the focus of the following survey, while bots and robots, while equally interesting, are beyond the scope of the current paper.

According to a dictionary, the word "Avatar" means: "embodiment: a new personification of a familiar idea"; or the manifestation of a Hindu deity (especially Vishnu) in human or superhuman or animal form. In an on-line community, Avatar is a virtual representation of a player in an on-line world, a software creation that exists in virtual environment but is controlled by a human player from the physical world. A comprehensive summary of avatar types is given in an on-line book by John Suler, Department of Psychology Professor at Rider University [55]. The book itself is not your ordinary collection of printed articles – it exists only in the on-line form and evolves with time to reflect constant changes in virtual gaming communities. According to [55], the following types of avatars exist based on preferences and behavior of its human creator:

Odd/shocking avatars are unusual, strange, or bizarre; Abstract avatars may be represented by abstract art; Billboard avatars are announcements of some kind; Lifestyle avatars depict a significant aspect of a person's life; Matching avatars are designed to accompany each other; Clan avatars are worn by members of the same social group; Animated avatars contain motion; Animal avatars are typically associated with person's pets or self association with nature; Cartoon avatars are based on famous drawn characters; Celebrity avatars tend to follow trends in popular culture; Evil avatars are scary looking; Real Face avatars are uploaded pictures of the actual users; Idiosyncratic avatars are strongly associated with a specific user; Positional avatars are designed by the member to be placed into specific locations; Power avatars are symbols of omnipotence; Seductive avatars partially naked or scantily clothed figures.

Identification of such avatars can be carried out through analysis of their appearance, attributes, behavioral patterns, frequency and type of changes, using a combination of traditional image pattern recognition techniques and biometric behavioral identifiers. Classifying further the types of behaviors that avatars might exhibit can assist significantly in the task of avatar authentication. According to [55], such behavior can be expressed in Mischievous Pranks (such as smearing someone else's room, spoofing someone with "msay" command, or popping text balloon over someone's head), Flooding of the server by users who make rapid multiple changes of their avatars, Blocking (placing one's avatar on top or too close to another person's prop), Sleeping (by users who have walked away from their computer and their avatar fails to react), Eavesdropping (by reducing avatar to a single pixel and usernames to only one character, someone may become "invisible" and secretly listen in on conversations), Prop Dropping (placing an inappropriate or obscene prop in an empty room), Identity Disruption - people suffering from disturbances in their identity may act it out through frequently changing props they wear. Imposters - stealing someone's avatar, wearing it and also using that person's name (or a variation of it) – one of very serious crimes in cyberworld as it is essentially "stealing someone else's entire identity". Those behaviors resemble typical criminal behaviors of humans and so require high degree of attention from those in charge of security of the virtual communities.

Author of [55] describes one such act "Sometimes, it's hard even for sympathetic people to resist the antics and game-playing. One night, although trying to remain a neutral observer, I eventually found myself as an accomplice to another member in a prank where we set up an unmanned female prop in the spa pool. We used "msay" to talk THROUGH the prop while also talking to it as if it were another user. Essentially, it was a virtual ventriloquist act. Honey " (the prop) was rather seductive towards the guests, and the guests all thought it was a "real" person. It was quite funny, although perhaps a bit mean to the poor naive guests who were unaware of the msay command." The paragraph above is highly interesting as it describes the process of another virtual entity creation, or a "fake avatar", separate from legitimate avatars, that does not corresponds to a real person, but "appears" to be just like them and can sometimes fool even experienced users. Utilizing methods from biometric research as well as developing new approaches targeting specifically avatar authentication and behavior recognition can assist in identifying those "fake avatars" as well as classifying real ones.

4 Avatar Authentication

In this section, we first take a look at techniques for collecting and classifying databases of avatars and bots, moving on to propose a new way to synthesis the new images through application of biometric synthesis methods based on geometric processing and multi-resolution techniques. We then study the two main types of authentication in virtual world: visual and behavioral, and introduce the multi-resolution system for enhanced performance.

4.1 Datasets Generation

In the well-established fields such as biometrics, numerous standardized and publicly available datasets exist [49] making it possible to compare experimental results achieved by different algorithms and to test developed systems. Labeled public datasets of avatar faces, robot faces, or attributed conversations from artificially intelligent agents are currently unavailable. Techniques for creation of standardized and consistent with real world datasets can be learned from examining approaches to generation and evaluation of facial datasets [29, 15] utilized by biometric security systems or from chat mining research applied to gender attribution [9] and human versus bot classification [18].

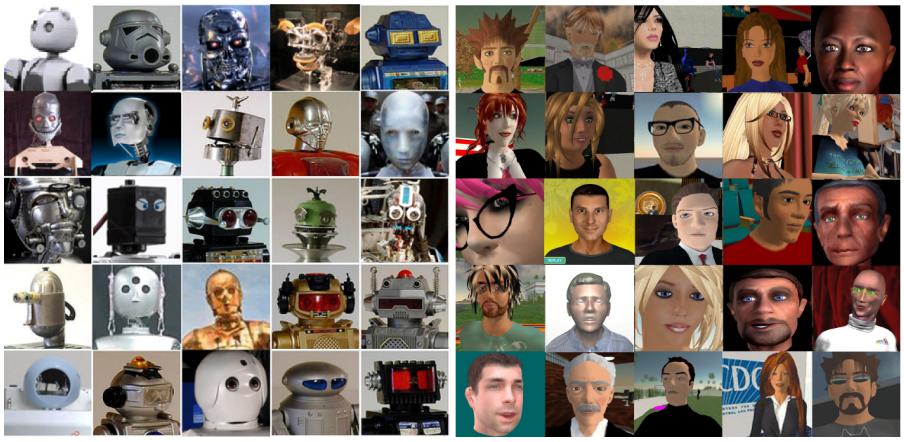

Fig. 2. *Left:* Sample images for a robot-face dataset, currently limited to manual collection; *Right:* Automatically generated random avatar-faces [43] [65]

The authors of this paper have begun work on generation of a publicly available avatar face dataset [43] by designed and implemented a scripting technique to automate the process of avatar face collection. Using the programming language AutoIt as well as a scripting language native to *Second Life*, better known as Linden Scripting Language (LSL), a successful generation of random avatars was achieved. The following is a walkthrough of this process for the creation of randomly generated dataset of avatar faces:

1) Using the scripting language AutoIt, it was possible to simulate key presses and mouse control in a Windows environment. During the first run of the AutoIt script, simulated keyboard commands are used to circle the *Second Life* camera around the avatar such that the front of the avatar's face is exposed.
2) The script is paused and requests the user to center the avatar's face with the horizon using the movement control. This is only needed on the first run and constitutes the last interaction with the user.
3) The AutoIt script then activates the LSL script by clicking on a button attached to the avatar's hub.

4) The LSL script locks the *Second Life* camera's position and rotation as well as controls from the game's automated functions (such as camera changing on clicking).
5) The AutoIt script then takes a screen shot of the avatar using the *Second Life* tool "screen shot". The script then labels avatar "Avatar 'x' face 'y'", where x corresponds to the number of avatar created (1 - N) and y corresponds to the screen shot for that avatar (1 – 10).
6) The script then zooms into the avatar's face before taking another screen shot and using the same labeling system as in step 5.
7) The AutoIt script then rotates the camera at eight specific angles (upper left, center left, lower left, upper center, lower center, upper right, center right, and lower right) taking screen shots at each.
8) The script then selects "edit", then "appearance", bringing up the avatar editing tool. From here the script randomizes a body for a new avatar. Body height, torso length, and leg height all must be set to 50% in order to preserve the camera angle, which is done automatically by the script.
9) The AutoIt script then clicks on the body parts sub menu items "skin", "hair", and "eyes" randomizing each of them as they are entered. The save "all button" is pressed, saving the avatar to begin the screen shot process again.
10) The script zooms away from the avatar before taking the new avatar's center body screen shot.

After step 10, the AutoIt script restarts at step 7 until all the images have been taken. A sample segment of Autoit source code responsible for GUI interaction is given below [43]:

```
Func snapshot ($picture)
dim $picture
mouseClick("Left", 440, 756, 1)   ;snapshot button
sleep(2000)
mouseClick("Left", 102, 296, 1)   ;save button
sleep(3000)
send("{DOWN}{ENTER}")
findname($picture)                    EndFunc
```

The datasets generated by the scripted approach consists of ten pictures for each avatar taken from different angles. The images captured are in the Portable Network Graphics (PNG) format at a resolution of 1024 X 768 resulting in each image being between 110KB and 450KB in size. One upper body picture is taken as well as nine facial pictures, all differing in angles. These angles include the top, center, and bottom of the left, center and right side of each avatar's face. The images are named in a consistent format; stating the program, gender, avatar number, and angle. For example, the image "SecondLife Male Avatar 4 gesture 5.png" refers to the image of an avatar that looks like a male character, the fourth in the dataset, and the fifth picture taken in this avatar's set of 10. The gender of the avatar is dependent upon the user's selection at the beginning of the process.

In a separate project we are also working on collection of speech corpora from intelligent agents. We are assembling a a text corpus from intelligent agents who have performed extremely well in the recent Lobner.net prize in Artificial Intelligence

competitions. With the assistants of the developed tools any researcher in the field can effortlessly generate virtually unlimited amount of data for visual and stylometric robot authentication experiments.

Currently, it is only possible to specify the desired amount of data and the gender of the avatars' faces and overall area of knowledge about which intelligent agents communicate. It is however already possible to generate multiple samples for each non-biological entity making it easy to perform training and testing on disjoint datasets. Additional work is still necessary to make it possible to generate data with specific characteristics, in which we propose to utilize some of the recently developed biometric synthesis processes as outlined below.

4.2 Synthetic Biometric and Artimetrics

A link between two areas - avatar generation and synthetic biometric generation, is very weak at the moment. One of the first examples can be accredited to 1998 report "*Avatar Creation using Automatic Face Recognition",* where authors discuss specific steps and processing techniques that need to be taken in order for avatar to be created almost automatically from a human face [36]. However, authors of this article postulate that the process of avatar creation and authentication can be further augmented by applying techniques from both biometric synthesis and biometric authentication.

Synthetic biometric is defined as "inverse problem of biometric" [70] and is intended to create artificial phenomenon that does not exist in physical reality, but resembles it. The extensive research on synthetic biometric has been conducted at the Biometric Technologies Laboratory, University of Calgary, and results has been recently reported in the World Scientific book "Image Pattern Recognition: Synthesis and Analysis in Biometrics" [69]. In that study, link between biometric synthesis and inverse logic has been established, as the same principles can be applied to solve inverse logical problems and generate new synthetic biometric data. There are numerous applications and high demand for new biometric databases to test new systems and study various phenomena, and many novel methods based on feature selection, pattern analysis, functional decomposition of spaces, signal processing, image decomposition and multi-resolution has been employed to generate new synthetic biometric data. However, looking at the problem from another point of view, synthetic biometric creations such as fingerprints, irises, faces, ears, hands, behavioral trends and virtual bodies are similar to avatars. They are created artificially, using computer means and sophisticated algorithms, to resemble human and human features. However, there are some substantial differences that make synthetic biometric be recognized in their own category. This is discussed next.

Synthetic biometric, at least up to day, is completely non-personalized. It usually does not correspond to a single human or function, but possesses characteristics of multiple biometrics that were used in the process of new biometric entity synthesis. However, exactly this property might prove most beneficial for new virtual dataset creation. In general, data synthesis refers to the creation of new data to meet some intended purposes, and includes areas such as texture synthesis, domain specific rendering and biometric synthesis. Due to logistical and privacy issues with collecting and organizing large amounts of biometric data, a new direction of biometric research concentrates on the synthesis of biometric information. One of the primary goals of

the synthesis of biometric data is to provide databases for testing newly developed biometric algorithms [17]. For instance, author of this paper proposed an approach for facial synthesis and expression modeling based on the underlying mesh modification for both 2D and 3D face models. Selection of control points in this method is guided by the three-dimensional Voronoi diagram which represents the [72]. A general overview of related work on utilizing geometric algorithms in facial expression modeling can be found in [16].

However, not all synthetic biometric comes from multiple sources. While opportunities for customization and specific feature selection are endless when creating a new synthetic data, some data, such as synthetic face, might be created based on a single source – a single photograph or face drawing. The source in this case can be both real (actual photograph or a face scan) or artistically created (cartoon character, caricature etc.), but the resulted synthetic face can resemble the source and have its own personally customized features. For example, one can create a facial image in any pose, with chosen illumination, given color of the eyes, selected hair style and accessories (mustache, glasses, beard etc). Moreover, a concept of time can be introduced and the same synthetic face can be of a young person, middle-aged individual or an old human. The same is true for an avatar – it can resemble its creator, but is fully customizable in appearance, gender, age, voice or interaction with other characters. Thus, it is only natural to make a link between biometric synthesis studies and avatar creation and recognition domain, which is the scope of artimetrics.

4.3 Visual Recognition

We now would like to concentrate specifically on visual recognition of avatars problem. Face Recognition is the task naturally performed by humans, and it remains in the center of biometric research over the last few decades. Hundreds of papers have been published on the topic, with comprehensive surveys of facial biometric research found in [68, 73, 56] as well as in a recent book presenting state-of-the-art in the area [23]. Dozens of different approaches ranging in accuracy of face recognition from low 60% to 99% have been proposed [68]. Knowledge based methods, such as the multi-resolution based approach [67], capture the relationship between facial features. Feature invariant approaches look for structures consistency under a variety of poses and lighting conditions, examples include grouping of edges [71], space gray-level dependence matrix [11], and mixture of Gausians [38]. Template matching extracts standard patterns of the face which are later compared to regions being tested to determine the degree of correlation, classical examples include shape template [10] and Active Shape Model [34]. Finally, appearance-based methods such as Eigenvector decomposition [60], Support Vector Machines (SVM) [42], Hidden Markov Model [45], Naïve Bayes Classifier [50] and Neural Networks [48] learn facial templates from a set of training image.

It is interesting to note that the performance of such adapted technique on avatar face recognition would be superior to method performance among humans. Consider an actual scene in the natural world. The effects of air quality, lightning, reflections, person's posture, clothing, and possible movement, as well as the type of the physical medium used to capture the image (film, camera, cell phone) and the distance/positioning of this capturing device from the person make the problem of face

recognition extremely difficult and not resolved up to date. However, in the virtual world, while some variability still exists, the nature of the avatar being a computer generated entity makes it much easier to extract the "ground truth" - the way avatar face was initially created, and thus to develop a standardized approach to avatar face recognition. An example of application of feature-based (geometry-based) method to avatar recognition is given in Figure 3 below.

Fig. 3. Feature-based facial recognition applied to an avatar's face

Another important fact to consider is that, as mentioned in the introduction, some research confirms a strong resemblance of avatar to its human creator, which makes it possible to use the results of successful avatar recognition for human recognition, and vice versa. This will, in turn, open a new area of *virtual biometric*, or augmenting the actual biometric with results of recognition in virtual world.

4.4 Behavioral Authentication

As mentioned above, facial recognition, alone with expression analysis and face synthesis, are highly prominent and actively researched areas of biometric [17, 23]. Facial expression analysis has been an active research topic for behavioural scientists since the work of Darwin in 1872. Emotion recognition was studied in paralinguistic communication, clinical psychology, psychiatry, neurology, pain assessment, lie detection, intelligent environments, and multimodal human-computer interface (HCI). From comprehensive book chapters devoted to state of the art research on facial expression and modeling, to tutorials in Biometric conferences and Biometric conference themes devoted exclusively to face animation, morphing, expression analysis and 3D models - the area is receiving a spur of attention from biometric communities, consortiums and industries worldwide. One of the emerging recent trends is capturing subtle details such as wrinkles, creases and minor imperfections that are highly important for biometric modeling as well as matching.

A novel approach to the problem recently introduced to the scientific community takes into an account subtle expression changes and performs morphing expression images in 2D and 3D based on the powerful computational geometry methods [72]. This work makes a number of important contributions to the field of expression modeling and morphing: it is one of the first applications of the sketch-based approach to facial image generation and the first one that preserves and utilizes subtle expression lines. It provides a simple fully automated algorithm based on the distance transform that computed the mapping between pixels in a monochrome image through a clever process of sweeping the image and reusing the information obtained on the previous step. It also provides a combination of Sibson coordinates and Delaunay triangulation mesh to generate and morph 3D facial models. Because all the generated facial models have the same underlying structure, animation created by developed tools can be easily retargeted to various models. Thus, it allows generating facial models with different expressions suitable for further utilization in biometric testing and behavioral research.

Forensics and more specifically authorship recognition, sometimes called stylometry, is another area related to *behavior-based authentication* of identity. In particular, a lot of research has been done in vocabulary analysis and profiling of plain text [25, 32, 33], emails [54, 61] and source code [51, 19, 14]. Written text or spoken word, once transcribed, can be analyzed in terms of vocabulary and style to determine its authorship. In order 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 or item distribution through a text [20]. 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 [52]. Once linguistic features have been established Support Vector Machines [24], Bayesian classifiers [28], multiple regression and discriminant analysis [53] algorithms (among others) have been applied to determine the authorship of the text. Applying the techniques above to pattern recognition and behavior authentication of avatars based on the way they present themselves, perform their tasks, and communicate in the virtual world is another emerging area of research.

4.5 Multi-modal Systems for Avatar Recognition

Biometric system based solely on a single biometric may not always identify the entity (human or avatar) in the most optimal or precise way. Thus, multibiometric system research is emerging as a trend which helps to overcome limitations of a single biometric solution [47]. This is especially useful in the presence of complex patterns, conflicting or misleading behavior, abnormal data samples, intended or accidental mischief etc. 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 [47], thus enhancing security and performance of authentication system.

Multimodal biometric approaches improve overall system accuracy and address issues of non-universality, spoofing, noise, and fault tolerance. Multimodal biometrics can referrer to a number of different approaches such as [46]:

- Multi-Sensor – employ multiple sensors to capture a single biometric trait.
- Multi-Algorithm – utilize a number of feature extraction or matching algorithms on the same data.
- Multi-Instance – utilize data from multiple instances of the same trait such as multiple fingerprints Multi-Sample – collect multiple instances of the same trait via a single sensor.
- Multi-Modal – utilize multiple biometric traits (ex. face and fingerprint and voice).

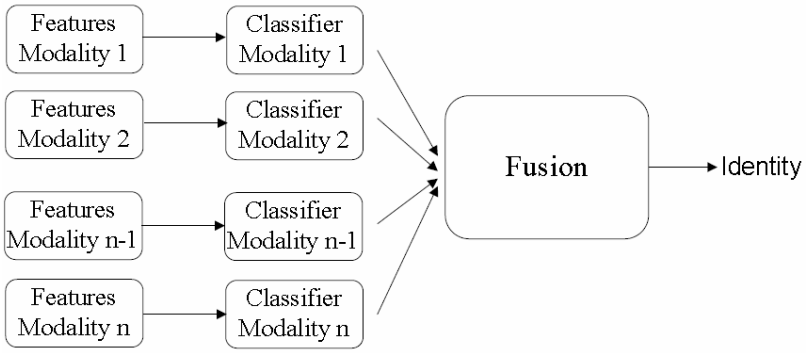

Fig. 4. An example of a multi-modal system architecture

An example of multi-modal biometric system architecture is shown in figure 4. Here, features and classifiers can be obtained from single biometric but acquired but multiple sensor devices, from multiple biometrics (i.e. physiological or behavioral), or from both single and multiple biometrics (with various acquisition, pre-processing and feature extraction techniques). The results of classification are then fused to determine the identity, and this type is generally referred to as post-classification fusion. An architecture will be different for fusions methods.

In a similar manner, together behavioral and physical artimetrics in the virtual worlds can be utilized as a part of a Physoemotional Artimetric system which is a multimodal system. In fact, this approach could be particularly beneficial for artificial entities recognition as there are more ways to "disguise" yourself in the virtual world than in the real world. For example, plastic surgery to change someone's appearance might be an expensive, time consuming and risky way to forge identity of an individual, but changing avatar appearance is much easier, cheaper and faster. Thus, behavioral traits in the virtual world start to play a much more important role. While appearance recognition value somewhat diminishes, the behavior pattern study, popular activities analysis, social surroundings, manner of speech, favorite places to visit, hobbies, skills, art and even wealth in virtual world can supply the crucial information for virtual entity authentication. Combining the visual and behavioral artimetrics

using multi-modal biometric approach is emerging area of research that we introduce. In addition, we introduce another concept of Multi-Dimensional system, crossing over between virtual and real world. The concept proposes visual authentication of avatar through its creator authentication, and vice versa, in both virtual and real domains.

5 Applications

There are numerous applications for the methodology, some of which are listed below.

One is preventing malicious intelligent software from obtaining access to information or system resources and granting it to authorized agents. By doing so, one can improve security of virtual communities, social networks, and country's cyber-infrastructure especially vulnerable in the post 9/11 world.

With exponential growth in abilities of artificially intelligent agents (bots, software weapons, viruses, etc.) comes the pressing need to secure information and resources from access by the unauthorized agents, while at the same time allowing seamless access for the "goodware". Behavior based profiling of software agents provides an unobtrusive way of separating helpful bots from malware. Additional research in artimetrics is likely to produce novel behavior-profiling approaches specifically designed to take advantage of the unique "psychology" of artificially intelligent programs. Current explosive research on CAPTCHAs [66, 1, 3, 4, 39] demonstrates one promising direction of future research.

Finding out which agent has performed a given task in case a number of possible alternatives exist, either for demanding responsibility or assigning reward, is another application area. Behavioral profiling can be used to uniquely identify a specific type of avatar and potentially the avatar owner. Examples of such 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 matched up with known behavioral signatures leading to attribution of the attack to a particular hacker or a mischievous group.

Securing interaction between different pieces of intelligent software or between a human being and an instance of intelligent software in a virual world is also an important domain [30, 26]. Botnents, groups of intelligent cooperating agent and mixed robot/human teams are quickly emerging in numerous domains. Being able to secure their communications is important for further progress in e-commerce, crowdsourcing, virtual community development, construction, military and any other industry with heavy reliance on team based efforts. In order to communicate securely identity of all parties wishing to exchange information needs to be determined with high degree of accuracy. Consequently, it is important to develop automatic algorithm which would give robots ability to recognize other robots and human beings they are working with. While numerous algorithms exist to authenticate identity of specific robots/computers based on digital signatures and cryptographic networking protocols in human dominated environments, robots have a better chance of "fitting-in" if they utilize humanlike biometric approach to identity management advocated in this paper.

Other applications include detecting cheating in games based on assistance from AI software, for example in chess, provide visual and behavioral search capabilities

for the virtual worlds, such as Second Life, based on descriptions of individuals, and targeting merchandise marketing in virtual worlds only to agents matching a certain profile.

6 Conclusions and Future Work

This review paper describes 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 builds on and expands such diverse fields of science as forensics, robotics, stylometry, computer graphics, biometrics and security. The paper describes how verification and recognition of avatars can be carried out via visual properties and behavioral profiling. It also introduces a multimodal system, simultaneously profiling multiple independent physical and behavioral characteristic of en entity, and postulates the feasibility of creating a multimodal system capable of authenticating both biological (human being) and non-biological (avatars) entities.

Potential directions for future Artimetrics research include the investigation of other visual and behavioral approaches to avatar/robot security based on appearance of new characteristics and abilities in the avatars/robots of tomorrow. Even today it is possible to expand robotic biometrics beyond faces and vocabulary to intelligent software agents which mimic higher order human intelligence (such as composing inspiring music, drawing beautiful paintings, and writing poetry). As AI and virtual reality research progresses, it will in turn stimulate creation of new security solutions to identity management across both human and artificial entity worlds.

Acknowledgments. The authors would like to acknowledge the contributions of the members of Biometric Technologies Laboratory (BTLab) at the University of Calgary, as well as Prof. Alexei Sourin for his valuable help in manuscript preparation. The authors also would like to acknowledge the support of NSERC Funding Agency, Canada.

References

[1] L., Ahn, L.v., Blum, M., Hopper, N., Langford, J.: CAPTCHA: Using Hard AI Problems for Security, Eurocrypt (2003)

[2] Asoh, H., Hayamizu, S., Hara, I., Motomura, Y., Akaho, S., Matsui, T.: Socially embedded learning of the office-conversant mobile robot jijo-2. In: 15th International Joint Conference on Artificial Intelligence, IJCAI (1997)

[3] Baird, H.S., Bentley, J.L.: Implicit CAPTCHAs. In: Proceedings of the SPIE/IS&T Conference on Document Recognition and Retrieval XII (DR&R2005), San Jose, CA (January 2005)

[4] Bentley, J., Mallows, C.L.: CAPTCHA challenge strings: problems and improvements, Document Recognition & Retrieval, January 18-19 (2006)

[5] Boyd, R.S.: Feds thinking outside the box to plug intelligence gaps, `http://www.mcclatchydc.com/2010/03/29/91280/feds-thinking-outside-the-box.html` (retrieved April 10, 2010)

[6] Charles, J.S., Rosenberg, C., Thrun, S.: Spontaneous, Short-term Interaction with Mobile Robots. In: IEEE International Conference on Robotics and Automation, pp. 658–663 (1999)
[7] Chen, K.-J., Barthes, J.-P.: Giving an Office Assistant Agent a Memory Mechanism. In: 7th IEEE International Conference on Cognitive Informatics (ICCI), Compiegne, pp. 402–410 (2008)
[8] Cole, J.: Osama bin Laden's Second Life, Salon, (2008) http://www.salon.com/opinion/feature/2008/02/25/avatars/ (retrieved June 7, 2009)
[9] Corney, M., Vel, O.d., Anderson, A., Mohay, G.: Gender-preferential text mining of e-mail discourse. In: 18th Annual Computer Security Applications Conference, Brisbane, Australia, pp. 282–289 (2002)
[10] Craw, I., Tock, D., Bennett, A.: Finding Face Features. In: Second European Conference on Computer Vision, Santa Margherita Ligure, Italy, pp. 92–96 (1992)
[11] Dai, Y., Nakano, Y.: Face-Texture Model Based on SGLD and Its Application in Face Detection in a Color Scene. Pattern Recognition 29(6), 1007–1017 (1996)
[12] Fisher, R.: Avatars can't hide your lying eyes, New Scientist, vol. (2755) (April 8, 2010), http://www.newscientist.com/article/mg20627555.600-avatars-cant-hide-your-lying-eyes.html
[13] Fong, T.W., Nourbakhsh, I., Dautenhahn, K.: A survey of socially interactive robots. Robotics and Autonomous Systems 42, 143–166 (2003)
[14] Frantzeskou, G., Gritzalis, S., MacDonell, S.: Source Code Authorship Analysis for Supporting the Cybercrime Investigation Process. In: 1st International Conference on eBusiness and Telecommunication Networks - Security and Reliability in Information Systems and Networks Track, pp. 85–92. Kluwer Academic Publishers, Setubal Portugal (August 2004)
[15] Gao, W., Cao, B., Shan, S., Chen, X., Zhou, D., Zhang, X., Zhao, D.: The CAS-PEAL Large-Scale Chinese Face Database and Baseline Evaluations. IEEE Transactions on Systems, Man and Cybernetics 38(1), 149–161 (2008)
[16] Gavrilova, M.L.: Algorithms in 3d real-time rendering and facial expression modeling, 3IA'2006 Plenary Lecture. Eurographics, 5–8 (May 2006)
[17] Gavrilova, M.L.: Computational geometry and image processing techniques in biometrics: on the path to convergence in Image Pattern Recognition. In: Synthesis and Analysis in Biometrics, World Scientific Publishers, Singapore (2007)
[18] Gianvecchio, S., Xie, M., Wu, Z., Wang, H.: Measurement and classification of humans and bots in internet chat. In: 17th Conference on Security Symposium, San Jose, CA, pp. 155–169 (2008)
[19] Gray, A., Sallis, P., MacDonell, S.: Software Forensics: Extending Authorship Analysis Techniques to Computer Programs. In: Proc. 3rd Biannual Conf. Int. Assoc. of Forensic Linguists, IAFL1997 (1997)
[20] van Halteren, H.: Linguistic profiling for author recognition and verification. In: Proceedings of ACL- (2004)
[21] Holz, T., Dragone, M., O'Hare, G.M.P.: Where Robots and Virtual Agents Meet. A Survey of Social Interaction Research across Milgram's Reality-Virtuality Continuum International Journal of Social Robotics 1(1) (January 2009)
[22] Ito, J.: Fashion robot to hit Japan catwalk, PHYSorg, http://www.physorg.com/pdf156406932.pdf (retrieved June 2009)
[23] Jain, A., Li, S.Z.: Handbook on Face Recognition. Springer, New York (July 2004)

[24] Joachim, D., Jorg, K., Edda, L., Paass, G.: Authorship Attribution with Support Vector Machines. Applied Intelligence, 109–123 (2003)
[25] Juola, P., Sofko, J.: Proving and Improving Authorship Attribution. In: Proceedings of CaSTA-04 the Face of Text (2004)
[26] Kanda, T., Ishiguro, H., Ono, T., Imai, M., Mase, K.: Multi-robot cooperation for human-robot communication. In: 11th IEEE International Workshop on Robot and Human Interactive Communication, pp. 271–276 (2002)
[27] Khurshid, J., Bing-rong, H.: Military robots - a glimpse from today and tomorrow. In: 8th Control, Automation, Robotics and Vision Conference (ICARCV), pp. 771–777 (2004)
[28] Kjell, B.: Authorship attribution of text samples using neural networks and Bayesian clas-sifiers. In: IEEE International Conference on Systems, Man, and Cybernetics. 'Humans, In-formation and Technology', San Antonio, TX, USA, pp. 1660–1664 (1994)
[29] Klimpak, B., Grgic, M., Delac, K.: Acquisition of a Face Database for Video Surveillance Research. In: 48th International Symposium focused on Multimedia Signal Processing and Communications, Zadar, pp. 111–114 (2006)
[30] Klingspor, V., Demiris, J., Kaiser, M.: Human-Robot-Communication and Machine Learning. Applied Artificial Intelligence 11, 719–746 (1997)
[31] Kobayashi, H., Hara, F.: Study on face robot for active human interface-mechanisms of facerobot and expression of 6 basic facial expressions. In: 2nd IEEE International Workshop on Robot and Human Communication, Tokyo, Japan, November 3-5, pp. 276–281 (1993)
[32] Koppel, M., Schler, J.: Authorship Verification as a One-Class Classification Problem. In: 21st International Conference on Machine Learning, Banff, Canada, pp. 489–495 (July 2004)
[33] Koppel, M., Schler, J., Mughaz, D.: Text Categorization for Authorship Verification. In: Eighth International Symposium on Artificial Intelligence and Mathematics, Fort Lauderdale, Florida (Januray 2004)
[34] Lanitis, A., Taylor, C.J., Cootes, T.F.: An Automatic Face Identification System Using Flexible Appearance Models. Image and Vision Computing 13(5), 393–401 (1995)
[35] Lim, H.-O., Takanishi, A.: Waseda biped humanoid robots realizing human-like motion. In: 6th International Workshop on Advanced Motion Control, Nagoya, Japan, pp. 525–530 (2000)
[36] Lyons, M., Plante, A., Jehan, S., Inoue, S., Akamatsu, S.: Avatar Creation using Automatic Face Recognition. In: ACM Multimedia 1998, Bristol, England, pp. 427–434 (September 1998)
[37] Lyu, M.R., King, I., Wong, T.T., Yau, E., Chan, P.W.: ARCADE: Augmented Reality Computing Arena for Digital Entertainment. In: IEEE Aerospace Conference, Big Sky, MT, March 5-12, pp. 1–9 (2005)
[38] McKenna, S., Gong, S., Raja, Y.: Modelling Facial Colour and Identity with Gaussian Mixtures. Pattern Recognition 31, 1883–1892 (1998)
[39] Misra, D., Gaj, K.: Face Recognition CAPTCHAs, International Conference on Telecommunications. In: Internet and Web Applications and Services (AICT-ICIW 2006), February 19-25, p. 122 (2006)
[40] Nood, D.d., Attema, J.: The Second Life of Virtual Reality., http://www.epn.net/interrealiteit/EPN-REPORT-The_Second_Life_of_VR.pdf (retrieved June 2009)
[41] Oh, J.-H., Hanson, D., Kim, W.-S., Han, I.Y., Han, Y., Park, I.-W.: In: International Conference on Intelligent Robots and Systems, Daejeon, pp. 1428–1433 (2006)

[42] Osuna, E., Freund, R., Girosi, F.: Training Support Vector Machines: An Application to Face Detection. In: IEEE Conference on Computer Vision and Pattern Recognition, pp. 130–136 (1997)
[43] : Parameterized Generation of Avatar Face Dataset. In: 14th International Conference on Computer Games: AI, Animation, Mobile, Interactive Multimedia, Educational & Serious Games, Louisville, KY (2009)
[44] Patel, P., Hexmoor, H.: Designing BOTs with BDI agents. In: International Symposium on Collaborative Technologies and Systems (CTS) Carbondale, USA, pp. 180–186 (2009)
[45] Rajagopalan, A., Kumar, K., Karlekar, J., Manivasakan, R., Patil, M., Desai, U., Poonacha, P., Chaudhuri, S.: Finding Faces in Photographs. In: 6th IEEE Intern. Conference on Computer Vision, pp. 640–645 (1998)
[46] Ross, A.: An Introduction to Multibiometrics. In: 15th European Signal Processing Conference (EUSIPCO), Poznan, Poland (September 2007)
[47] Ross, A., Jain, A.: Information fusion in biometrics. Pattern Recognition Letters 24, 2115–2125 (2003)
[48] Rowley, H., Baluja, S., Kanade, T.: Neural Network-Based Face Detection. IEEE Transactions on Pattern Analysis and Machine Intelligence 20(1), 23–38 (1998)
[49] Li, S., Jain, A. (eds.): Handbook of Face Recognition-Face Databases. Springer, New York (2005)
[50] Schneiderman, H., Kanade, T.: Probabilistic Modeling of Local Appearance and Spatial Relationships for Object Recognition. In: IEEE Conference on Computer Vision and Pattern Recognition, pp. 45–51 (1998)
[51] Spafford, E.H., Weeber, S.A.: Software Forensics: Can We Track Code to its Au-thors? In: 15th National Computer Security Conference, pp. 641–650 (October 1992)
[52] Stamatatos, E., Fakotakis, N., Kokkinakis, G.: Assoc. Computational Linguistics. In: Automatic authorship attribution, in Proc. nineth Conf. European, Bergen, Norway, pp. 158–164 (June 1999)
[53] Stamatatos, E., Fakotakis, N., Kokkinakis, G.: Computer-Based Authorship Attribution Without Lexical. Measures Computers and the Humanities 35(2), 193–214 (2001)
[54] Stolfo, S.J., Hershkop, S., Wang, K., Nimeskern, O., Hu, C.-W.: A Behavior-based Approach to Securing Email Systems. Mathematical Methods, Models and Architectures for Computer Networks Security 2776, 57–81 (2003)
[55] Suler, J.: The Psychology of Cyberspace, On-line book (2009), http://psycyber.blogspot.com
[56] Tan, X., Chen, S., Zhou, Z.-H., Zhang, F.: Face recognition from a single image per person: A survey. Pattern Recognition 39(9), 1725–1745 (2006)
[57] Tang, H., Fu, Y., Tu, J., Hasegawa-Johnson, M., Huang, T.S.: Humanoid Audio–Visual Avatar With Emotive Text-to-Speech Synthesis. IEEE Transactions on Multimedia 10, 969–981 (2008)
[58] Teijido, D.: Information assurance in a virtual world. In: Australasian Telecommunications Networks and Applications Conference (ATNAC 2009), Canberra, Australia, November 10-12 (2009)
[59] Thompson, B.G.: The State of Homeland Security, House.gov (2006), http://hsc-democrats.house.gov/SiteDocuments/ 20060814122421-06109.pdf (retrieved June 10, 2009)
[60] Turk, M., Pentland, A.: Eigenfaces for Recognition. Journal of Cognitive Neuroscience 3(1), 71–86 (1991)

[61] Vel, O.D., Anderson, A., Corney, M., Mohay, G.: Mining Email Content for Author Identification Forensics. ACM SIGMOD Record: Special Section on Data Mining for Intrusion Detection and Threat Analysis 30(4), 55–64 (2001)
[62] Yampolskiy, R.V.: Behavioral Biometrics for Verification and Recognition of AI Programs. In: 20th Annual Computer Science and Engineering Graduate Conference (GradConf), Buffalo, NY (2007)
[63] Yampolskiy, R.V.: Mimicry Attack on Strategy-Based Behavioral Biometric. In: 5th Interna-tional Conference on Information Technology: New Generations (ITNG 2008), Las Vegas, Nevada, April 7-9, pp. 916–921 (2008)
[64] Yampolskiy, R.V., Govindaraju, V.: Behavioral Biometrics for Recognition and Verification of Game Bots. In: The 8th Annual European Game-On Conference on Simulation and AI in Computer Games (GAMEON 2007), Bologna, Italy, November 20-22 (2007)
[65] Yampolskiy, R.V., Govindaraju, V.: Behavioral Biometrics for Verification and Recognition of Malicious Software Agents. In: SPIE Defense and Security Symposium, Orlando, March 16-20 (2008)
[66] Yampolskiy, R.V., Govindaraju, V.: Embedded Non-Interactive Continuous Bot Detection. ACM Computers in Entertainment 5(4), 1–11 (2007)
[67] Yang, G., Huang, T.S.: Human Face Detection in Complex Background. Pattern Recognition 27(1), 53–63 (1994)
[68] Yang, M.-H., Kriegman, D.J., Ahuja, N.: Detecting Faces in Images: A Survey. IEEE Transactions On Pattern Analysis and Machine Intelligence 24(1) (2002)
[69] Yanushkevich, S., Gavrilova, M., Wang, P., Srihari, S.: Image Pattern Recognition: Synthesis and Analysis in Biometrics. World Scientific Publishers, Singapore (2007)
[70] Yanushkevich, S., Stoica, A., Shmerko, V., Popel, D.: Inverse Problem of Biometric. CRC Press/Taylor&Francis, Boca Raton (2005)
[71] Yow, K.C., Cipolla, R.: Feature-Based Human Face Detection. Image and Vision Computing 15(9), 713–735 (1997)
[72] Yuan, L., Gavrilova, M., Wang, P.: Facial metamorphosis using geometrical methods for biometric applications. IJPRAI 22(3), 555–584 (2008)
[73] Zhao, W., Chellappa, R., Phillips, P.J., Rosenfeld, A.: Face recognition: A literature survey. ACM Computing Surveys 35(4), 399–458 (2003)