International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 2 Issue 1 2011

SECURE WEB MARKETING USING EAR BIOMETRICS

Girish Kumar,
Lecturer, ACET, India
girishvansh@gmail.com

ABSTRACT

The researches discuss if the ears are unique or unique enough to be used as biometrics. Ear shape applications are not commonly used, but we can use Ear Biometrics for authentication while using web marketing. In this paper we present the basics of using ear as biometric for person identification and authentication for web marketing. Also the error rate and application scenarios of ear biometrics are presented.

1. Introduction

In general, biometrics is the science of measuring physical properties of living beings.

"Biometrics is the automated recognition of individuals based on their behavioral and biological characteristics."
(ISO/IEC)

Biometric systems play a significant role in almost all the security aspects. As it uses human traits for the identification purpose which cannot be stolen or lost, they are proving to be a better solution than pins and passwords. There are many human traits that can be used as a biometric like fingerprint, face, signature, facial geometry, retina, hand geometry, finger geometry, vein structure of hand, voice, DNA, odor, keyboard strokes. It has been seen that finding two ears

which are completely identical is almost impossible and ear does not change much with time, unlike face. Moreover, ear satisfies all the properties that should be possessed by a biometric [2].

The ear has been proposed as a biometric. The difficulty is that we have several adjectives to describe e.g. faces but almost none for ears. We all can recognize people from faces, but we hardly can recognize anyone from ears.

2. Concept of Web Marketing

Internet marketing also referred to as i-marketing, web-marketing, online-marketing or e-Marketing, is the marketing of products or services over the Internet.

Internet marketing is associated with several business models:

- E-commerce – In this model, goods are sold directly to consumers (B2C) or businesses (B2B) or consumer to consumer(c2c)
- Lead-based Websites – Strategy where an organization generates value by acquiring sales leads from its website
- Affiliate Marketing – The process in which a product or service developed by one entity (e-commerce business, single person, or a combination) is sold by other active sellers for a share of profits. The entity of the product may provide some marketing material (sales letter, affiliate link, tracking facility), however, the vast majority of affiliate marketing relationships come from e-commerce businesses that offer affiliate programs.
- Blackhat Marketing – This is a form of Internet marketing that employs deceptive, abusive, or less than truthful methods to drive web traffic to a website or affiliate marketing offer. This method sometimes includes spam, cloaking within search engine result pages, or routing users to pages they didn't initially request.

3. Security Aspects for Web Marketing

Information security is important both to companies and consumers that participate in online business. Many consumers are hesitant to purchase items over the Internet because they do not trust that their personal information will remain private.

Some companies that purchase customer information offer the option for individuals to have their information removed from the database, also known as opting out. However, many customers are unaware if and when their information is being shared, and are unable to stop the transfer of their information between companies if such activity occurs.

Another major security concern that consumers have with e-commerce merchants is whether or not they will receive exactly what they purchase. Online merchants have attempted to address this concern by investing in and building strong consumer brands (e.g., Amazon.com, eBay, Overstock.com), and by leveraging merchant/feedback rating systems and e-commerce bonding solutions. All of these solutions attempt to assure consumers that their transactions will be free of problems because the merchants can be trusted to provide reliable products and services. Additionally, the major online payment mechanisms (credit cards, PayPal, Google Checkout, etc.) have also provided back-end buyer protection systems to address problems if they actually do occur.

4. Ear

The most famous work among ear identification is made by Alfred Iannarelli at 1989, when he gathered up over 10.000 ears and found that they all were different. Already at 1906 Imhofer found that in the set of 500 ears only 4 characteristics was needed to state the ears unique (Hoogstrate et al., 2000).

A biometric specialist company Bromba GmbH (2003) has compared different biometrics including ear shape. In the table 1 the constancy of different biometrics is compared. The reasons

for variation over time are e.g. growth, aging, dirt, and injury. In a good biometric there is as little as variation possible. According to table 1 ear biometrics based on ear form are averagely permanent: already used biometrics like iris, retina and DNA are more permanent than ear form. At the same level are e.g. fingerprint and hand geometry. Less permanent than ear form are e.g. signature, facial structure and voice.

On the concept of ear identification concept it is quite possible to use this mechanism for identification of particular person. We have scanning technology as well as programming tools like C# .net framework to achieve this goal. Moreover we have different software's which are able to identify different parameters regarding recognition of 9 points (3 sub points) related to ear part having distinguishable distance from the center of the ear like Matlab, even this software is quite able to differentiate illumination factors , color effects etc. due to bright light and dim light surroundings. With the help of these tools we can aid one more component for secure web marketing, which is in growing phase. Although we have certain beta version biometric authentication methods like yahoo mail server login with thumb authentication, but ear can play one more security factor for web marketing.

Table 1. The permanence of different biometrics over the time. The best permanence has most 0-symbols and the worst least. (Bromba GmbH, 2003)

Biometric Trait	*Permanence over time*
Fingerprint (Minutia)	ooooo
Signature (dynamic)	oooo
Facial structure	ooooo
Iris pattern	ooooooooo
Retina	oooooooo
Hand geometry	ooooooo
Finger geometry	ooooooo
Vein structure of the back of the hand	oooooo
Ear form	oooooo
Voice (Tone)	ooo
DNA	ooooooooo
Odor	oooooo?
Keyboard strokes	oooo
Comparison Password	ooooo

5. Ear Biometrics Methods

There are at least three methods for ear identification: (i) taking a photo of an ear, (ii) taking "earmarks" by pushing ear against a flat glass and (iii) taking thermogram pictures of the ear. The most interesting parts of the ear are the outer ear and ear lope, but the whole ear structure and shape is used.

The structure of ear does not changes over the time. The medical literature reports [4] that ear growth after the first four months of the birth is highly linear i.e. proportional.

The anatomy used for different parts of the ear is shown in the fig. 1.

Taking photo of the ear is the most commonly used method in research. The photo is taken and it is combined with previous taken photos for identifying a person. The earmarks are used mainly in crime solving. Even though some judgments are made based on the earmarks, currently they are not accepted in courts. The thermogram pictures could be one solution for solving the problem with e.g. hair of hat.

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 2 Issue 1 2011

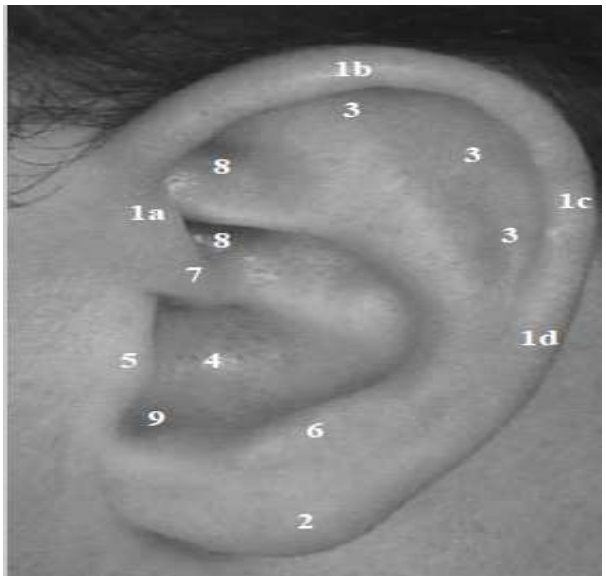

Figure 1 Anatomy of the ear

1. Helix Rim, 2 Lobule, 3 Anthelix, 4 Concha, 5 Tragus, 6 Antitragus, 7 Crus of Helix, 8 Triangular Fossa, 9 Incisure Intertregica [4]

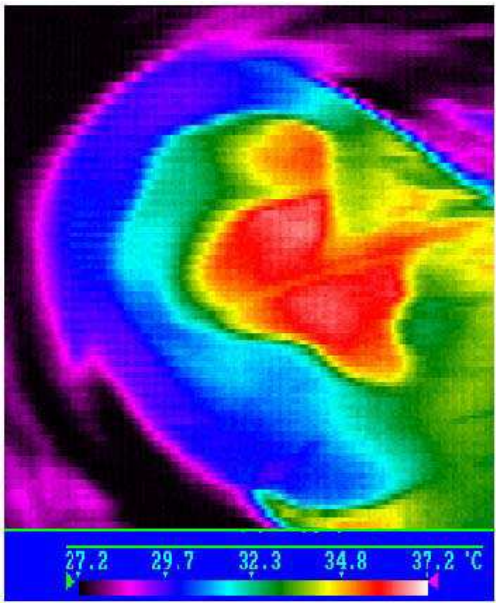

Fig. 2. Thermogram of an ear. Image provided by Brent Griffith, Infrared Thermography Laboratory, Lawrence Berkeley, National Laboratory. (Burge et al., 1998)

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 2 Issue 1 2011

6 PRINCIPAL COMPONENT ANALYSIS IN EAR RECOGNITION

Victor, Bowyer and Sarkar (2002) [3],have made a comparison between face and ear recognition. They used principal component analysis (PCA - Principal Component Analyzer, also known as "eigenfaces"), which is a dimensionality-reduction technique in which variation in the dataset is preserved. The classification is done in eigenspace, which is a lower dimension space defined by principal components or the eigenvectors of the data set.

The process consists of three steps:

i) Preprocessing, ii) Normalization, and iii) Identification (See figure 3 for more details).

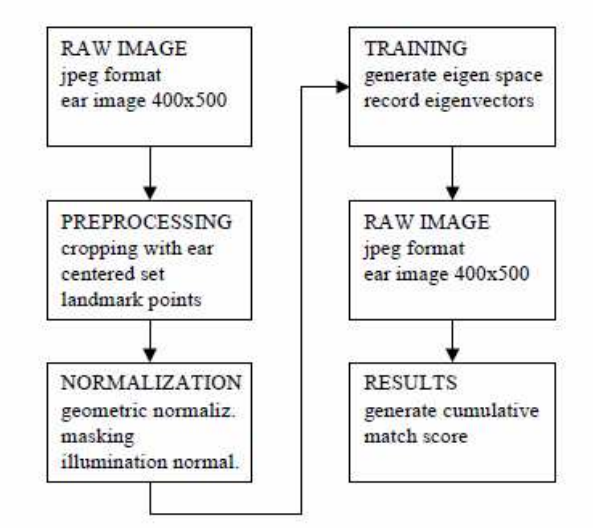

Fig. 3. Steps of PCA method.

7 APPLICATION SCENARIOS

There are several application areas where biometrics can be used either in identification or authentication. In identification the characteristic is compared with characteristics in a database for identifying who the person is. In authentication the characteristic of the person is in e.g. an ID card and this legal information is combined with the new one. (Ratha et al., 2001)

Biometrics can be used e.g. when collecting a child from daycare or boarding an aircraft or anything else between them (Ratha et al., 2001). A typical example of using biometrics is an

automatic teller machine (ATM). In this vision the user inserts the bankcard and types the personal identification number (PIN). Simultaneously the camera records the face and ear and the identity of the person will be supplementary verified. So not only the bankcard and the PIN have to be compatible with each other, but also the used biometrics have to fit in. (Burge et al. 1998)

Passive ear biometrics are ideal with different security levels. Currently access rights are handled mainly with different kinds of identity cards with passive transmitters. Anyone who gets the card can use it. In some cases there can be video cameras, which record the people who use the card. However it is not real time system. Using passive ear biometrics no person is allowed to enter restricted area without recognition the person. In the case two attempts of identification do not match, a camera is activated and linked to the security counsel's office. The security personnel can visually combine the picture in the database and the taken picture and decide if the person is allowed to enter to the restricted area. (Burge et al., 1998)

Hoogstrate et al. (2000) have researched the ability to identify a person from surveillance videotapes. There were many robberies of gas stations in The Netherlands. The offender was wearing a baseball cap, shawl and a cloth hanging from the cap to his face so that the face was covered. However the ears were visible. This is the fact that raised the question is people can be identified just from ear. The quality of the videotapes is increasing, which supports the possibility to use ear identification.

Applications using biometrics are more secure than traditional user name and password combinations. A requirement for personal identification systems is cost effectiveness: the systems should work with standard video and computer hardware. An advantage compared with e.g. retinal and iris scan is that ear recognition is less intrusive. (Moreno et al. 1999)

Biometrics is the cutting edge of security. Biometric Fingerprint Scanners offer a high security solution to identity theft from a stolen laptop computer.

There are several choices available for laptops with biometric fingerprint scanners. IBM offers several of the Lenovo models with the built in devices. Sony's Vaio and the Acer Aspire series

ISSN (Online) : 2229-6166

Volume 2 Issue 1 2011

both offer the scanner as an option. The new Alienware M17 also comes equipped with a fingerprint reader. These are all readily available and offer not only the reader and the software suite but also deliver great tutorials on how and when to use the system.

Laptop Computers that come with fingerprint scanners standard:

- Lenovo SL500 ThinkPad
- Lenovo T500 ThinkPad
- Acer Aspire 4736
- Acer Aspire 6920G
- Acer Aspire 3935
- Alienware M17
- Sony Vaio BX
- Dell XPS M1530
- Dell Latitude E6400/6500
- Toshiba Satellite P105-S6114
- Toshiba M400
- Gateway E-155C
- Gateway E-475m
- HP Compaq 6910p
- HP Compaq nc6400

When using biometrics for authentication purposes there are several viewpoints to taken into account. The system has to be Comfort, which means that the duration of the verification has to be as low as possible and the system must be easy to use. It also has to be Accurate so that the error rate is as low as possible. The system has to be Available when needed and where needed. The Costs of the system affects also to the use of biometric system.

8 Error Possibilities in Ear Identification

There are several error possibilities in ear identification. Basically the human ear shape is the same during the whole life and the growth is proportional. However, the gravity can cause ear stretching. The stretching is about five times greater from age of four months to age of eight years and again after about 70 years [2]. The ear can be covered e.g. with hair or a hat. Also the lightning and pose variation can cause error situations. In identification the idea is to check if the biometrics extracted from the picture sufficiently matches with the previously acquired ones. Because there are changes in the environment and the subject, some tolerance has to be accepted. This tolerance can be defined in terms of false reject rate (FRR) and the false acceptance rate (FAR), exhibited by the system. Usually one of the two is trying to be minimized depending on the required security level.

9 Conclusions

In conclusion, one may add that though ear is

still an infant in the ever enlarging field of biometrics. As the revolutionary advancement progresses in technology day by day, so ear biometrics in web marketing is quite valuable technique for secure web marketing.

10 References

[1] M. Burge, and W. Burger, Ear biometrics for machine vision, In 21st Workshop Austrian Association for Pattern Recognition, 1997.

[2] A. Iannarelli, Ear Identification, Forensic Identification Series, Paramount Publishing Company, 1989.

[3] An Evaluation Of Face And Ear Biometrics, Barnabas Victor, Kevin Bowyer, Sudeep Sarkar, 1051-4651/02 IEEE

[4] Alfred Iannarelli, Ear Identification, Forensic Identification Series, Paramount Publishing Company Fremount, California,1989

http://www.wikipedia.org

http://www.howstuffworks.com