WEBBIOMETRICS: USER VERIFICATION VIA WEB INTERACTION

H. Gamboa[*], *A. L. N. Fred*

Instituto de Telecomunicações,
Instituto Superior Técnico
Lisboa, Portugal

A. K. Jain

Michigan State University
East Lansing, Michigan

ABSTRACT

We introduce a biometric trait based on the user behavior extracted from his interaction with a web page. We propose the integration of this soft biometric trait in a conventional login Internet page to enhance the security of the system. We call this security layer *WebBiometrics*. This layer monitors the user mouse movements while he clicks his PIN code numbers. The proposed biometric method provides a non-intrusive soft behavioral biometric add-on to enhance on-line security. We describe the functionality of the system, the set of algorithms developed for the verification framework and preliminary experimental results. We also present quantitative measures of security enhancement offered by the introduction of this soft biometric compared to a PIN only based web access.

1. INTRODUCTION

There is a growing interest in major IT companies to capture the user behavior during web interaction. The analysis of the on-line user behavior is often referred to as Behavioral Targeting, a technique used to increase the results of marketing campaigns by directing the advertisement based on the user behavior. Google has patented [1] an algorithm that utilizes the behavior of the user to better classify the web pages and to direct the advertisement. Yahoo was the first company to launch a service based on Behavioral Targeting [2].

Human behavior has been used to develop several biometric authentication approaches as well. Handwritten signature [3] is one of the early biometric identification techniques in our society. Although establishing the authorship of handwritten signatures is somethimes difficult, human verification is normally very accurate in identifying genuine signatures. Biometric authentication based on on-line handwritten signatures relies on signature dynamics information to further reduce the possibility of fraud. Another behavioral biometric technique is speaker recognition via the voice print [4]. Despite some changes to the speakers' voice due to minor alterations caused by cough and cold, global speech characteristics such as user pitch, dynamics, and waveform analyzed using speech recognition techniques have been used successfully in several applications. Keystroke dynamics (or typing rhythms) [5] has also been shown to be a useful behavioral biometric technique. This method analyzes the way a user types on a terminal, by monitoring the keyboard input. The advantages of keystroke dynamics include the low level of detraction from the regular computer usage, because the user would be already entering keystrokes when entering a password in the system. Since the input device for this biometric is the existing keyboard, the technology has a lower cost compared to other biometric acquisition devices.

Over the Internet, the security protocols (without additional sensors hardware on the client side) generally do not have biometric verification modules. Some institutions that opened the Internet access to private and sensitive information such as baking institutions, had to enhance security and introduce some protection against automated attacks. This trend created interaction based login pages that aims at separating humans from computers (coined as CAPTCHA [6]), like the virtual keyboards with randomly positioned numbers used in several homebanking login pages. We propose the usage of the mouse movements dynamics to introduce an add-on module to the normal login and signin web pages, when the user has to introduce his PIN number, so that the user identity claim is verified. This system can be integrated in two additional scenarios: (i) In a continuous authentication system. The system monitors human computer interaction after the user has gained access to a system, continuously re-validating the identity of the user. (ii) As a complement to a hard biometric system (e.g. fingerprints). When the authentication process based only on the mouse movement in not reliable, a hard biometric trait could be requested to perform a second, more robust, authentication.

In this paper we present the WebBiomterics system based on the mouse movement while the user inserts the PIN number. This system implementation is based on our previous work on behavioral biometrics [7][8]. In section 2 we present the proposed WebBiometrics system. The overall system architecture is devised in section 3. We present experimental results in section 4. Section 5 presents a final discussion of the proposed system and plans for future work.

[*] This work was partially supported by the Luso-American Foundation Schoolarship #FDG094 and the grant FCT POSI/EEA-SRI/61924/2004

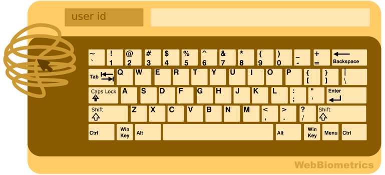

Fig. 1. Virtual keyboard presented to the user for id input.

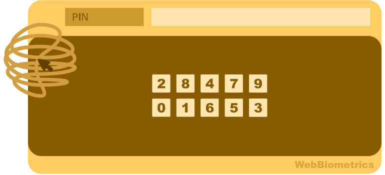

Fig. 2. The insertion of PIN code using a random numeric virtual keyboard.

2. WEBBIOMETRICS

The WebBiometrics system is used in a web environment in the context of a login page. The format of the login page is similar to some of the login setups used for low level security access that are designed to prevent automated machine based login. This login page has an embedded *virtual keyboard* that requests the user to click on the corresponding symbols in the figure of a keyboard (alphanumeric or numeric) presented on the web page. A first alphanumeric virtual keyboard asks the user to insert the *user id* (see Figure 1). A second *virtual keyboard* is presented with randomly ordered digits (see Figure 2), where the user clicks to compose his PIN code.

Inserting a PIN in a virtual keyboard with randomly ordered numbers introduces robustness to automated attacks. Even if the user interaction is recorded, it can not be replayed, given that the digits appear in distinct positions in every login attempt.

In every security system when an account is created there is always a signin or enrollment process, where some data is collected from the user. Given the type of information we are considering, namely the mouse movement behavior, we collect user data in a non conventional format. We use a virtual keyboard to fill a form during account creation.

The enrollment form is used to collect data like name, e-mail, address and some general information about the user. The PIN code is similar to a password but is composed only of digits. In order to collect behavioral information from PIN clicking, the user is asked to provide the PIN three times (it's a standard procedure to ask the user to insert a code twice in a normal sign in procedure in order to guarantee that there are no errors in the selected password).

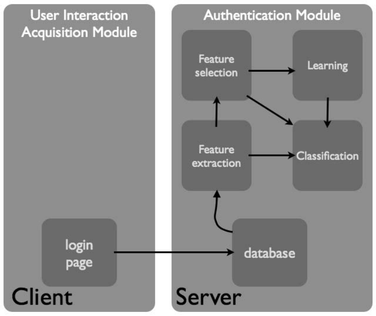

Fig. 3. WebBiometrics system architecture.

3. SYSTEM ARCHITECTURE

Our WebBiometrics system is based on a client-server architecture implemented over the Internet. The user will access a web-page on his computer (client) that transmits information to the remote authentication system (server). Figure 3 presents the building blocks of the WebBiometrics system composed of: (a) acquisition module; (b) feature extraction; (c) feature selection; (d) parametric learning; and (e) statistical sequential classifier. Each of the modules and it's internal workings are described in the next subsections.

3.1. Acquisition module

The acquisition system is called *Web Interaction Display and Monitoring*, WIDAM (for details, see [8]). It was developed by the authors to enable the remote visualization of a user activity in a page and record this information for playback purposes or to capture real time behavioral information about the user.

The WIDAM system allows the usage of an interaction recording system directly over a web page, based on the World Wide Web Consortium (W3C) standard Document Object Model (DOM) [9] that defines a web page. The system works in a normal web browser with java and javascript, without the need of any additional software installation. When the users accesses a page monitored by the WIDAM system, an applet is launched. This applet creates an Internet socket connection that enables message passing from, and to the server using a proprietary protocol developed for this purpose.

The format of the WIDAM recorded data for each user is a list of events composed of: the id of the event; the time instant of the event; the coordinates of the mouse (x,y); the id of the DOM object where the event occurred; the key pressed (if any); the state of modification keys (control, shift and alt). Since our study is centered on the mouse movement, we used the event id to distinguish mouse movement and mouse clicks and the (x,y) coordinates.

To study the proposed behavioral biometric, we designed a game with similarities to the task of inserting a PIN code in an Internet login page. The memory game is composed of a grid of tiles, each tile having associated a hidden pattern, which is shown to the user for a brief period of time upon clicking on it; the purpose of the game is to identify the matching tiles. The idea behind the selection of this game is that users are more cooperative in data collection if done in a game like environment than in a situation where we simply ask a user to click on numbers in a web page. The game is shown in figure 4. Figure 5 shows a graph of a user interaction recorded with WIDAM system while he is playing the entire memory game.

The graph is produced by joining every sequential mouse movement with lines and using a plus mark to indicate a mouse click.

3.2. Feature Extraction

The recorded data (Figure 5) is used to extract relevant features for the authentication module. A pattern in our system is defined as the mouse movement performed between successive clicks, which we will call a *stroke*. The number of strokes is associated with the length of the PIN code given that the user will produce as many strokes as the number of digits in the PIN.

The interaction data files produced by the acquisition system pass a feature extraction procedure. We create a 63-dimensional vector, exploring both spatial (related to angle and curvature) and temporal (related to duration, position, velocity and acceleration) characteristics of the strokes. More details can be found in [7].

3.3. Learning

The classification rule assumes a statistical model for the feature vector. The learning phase consists of the estimation of the class-conditional probability density functions, $p(X)$, where X is the feature vector of a stroke, from each user's data. We consider that each user constitutes a pattern class. Assuming statistical independence between features, $p(X)$ factorizes into $p(X|\ user) = \prod p(x_i|\ user)$. We use the *Weibull* distribution as the parametric model for $p(x_i|\ user)$: $p(x|a,b) = abx^{(b-1)}e^{(-ax^b)})$. Given the data from one user and one feature, maximum likelihood estimates of the parameters a and b are obtained.

3.4. Classification

The data collected in the enrollment phase of each user is used to create a global set of extracted features. A user-specific "best" subset of features is selected, using the equal error rate as performance measure (feature selection block in figure 3). We used the Sequential Forward Selection (SFS) algorithm [10] that adds one feature at a time to the vector of previously selected features.

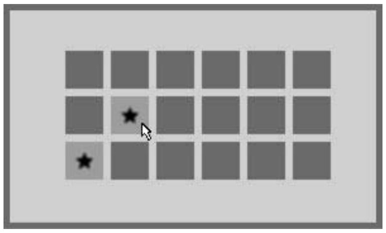

Fig. 4. The memory game; interaction page used for data collection. The game state after a pair of cards are matched.

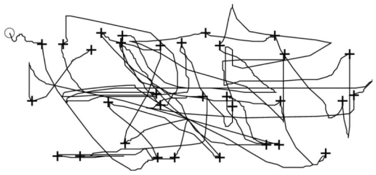

Fig. 5. Graph of the user interaction in a memory game.

The classifier verifies the identity of a user based on the patterns of interaction with the computer. Let the i^{th} user be denoted by the class $w_i, \quad i = 1, \ldots, L$, and L be the number of users. As defined before, a feature vector is associated with one stroke. Given a sequence of n_s consecutive strokes executed by the user, w_i, interaction information is summarized in the vector $\mathbf{X} = X^1 ... X^{n_s}$, consisting of the concatenation of the feature vectors associated with each stroke. $X^j = x_1^j ... x_{n_{f_i}}^j$, the feature vector representing the jth stroke, has n_{f_i} elements, n_{f_i} being the number of features identified for user w_i in the feature selection phase.

Considering one stroke at a time, and assuming statistical independence, between features we can write $p(X_j|w_i) = \prod_{l=1}^{n_f} p(x_l^j|w_i)$. Also considering stroke independence, we can further write $p(\mathbf{X}|w_i) = \prod_{j=1}^{n_s} p(X_j|w_i)$.

The classifier will decide to accept or reject the claimed identity based on two distributions: the genuine distribution $p(\mathbf{X}|w_i)$, and the impostor distribution $p(\mathbf{X}|\ \overline{w_i})$ that is based on a mixture of weibull distributions, one for each user under consideration, expressed as
$p(\mathbf{X}|\overline{w_i}) = \sum_{j \neq i} p(\mathbf{X}|w_i)\frac{1}{L}$. In the previous equation we assume that the classes are equiprobable, $p(w_i) = 1/L \quad i = 1...L$. We can, therefore, express the posterior probability function as $p(w_i|\mathbf{X}) = \frac{p(\mathbf{X}|w_i)}{\sum_{k=1}^{L} p(\mathbf{X}|w_k)} = 1 - p(\overline{w_i}|\mathbf{X})$.

Since $p(w_i|X_j)$ represents an estimate of the probability of the classification being correct, we establish a *threshold*, λ, to select one of the classes, using the decision rule in Eq. (1).

$$Accept(\mathbf{X} \in w_i) = \begin{cases} true & \text{if } p(w_i|\mathbf{X}) > \lambda \\ false & \text{otherwise} \end{cases} \qquad (1)$$

Table 1. Mean equal error rate (EER) and the standard deviation (SD) for different stroke sequence lengths (L).

L	EER	SD
5	0.17	0.07
10	0.12	0.06
15	0.06	0.04

4. RESULTS

Our results are based on a population 50 volunteers (engineering students) that used the system to play several memory games for about 10 minutes. This way, we created a repository of approximately 5 hours of interaction, containing more than 400 strokes per user. In order to use the same number of strokes per user in the tests, we randomly selected 400 strokes from each user. The set of strokes was divided into two equal parts, one for the training phase and the other for the testing phase. This separation assumes that we have access to approximately 4 minutes of user interaction while filling the signin forms in the enrollment phase, which we consider reasonable.

We applied the feature selection step using the test set, selecting a different set of features for each user. The performance measure used for feature selection was the classifier performance (EER) using sequences of 10 strokes.

When testing the system for one user, we considered an impostor as one of the other users. The test function returns the equal error rate given N sequences of strokes of length l using the classifier tuned for user i. The input sequence of strokes of a test is composed of $N/2$ strokes randomly sampled from the testing set of the user, and $N/2$ strokes randomly sampled from the testing sets of all the other users.

One of the free variables of the system is the number of strokes that the system will use in the verification task. Bootstrap [11] estimates of the system performance as a function of the sequence of several stroke lengths was obtained using 10,000 bootstrap samples from the test set. Table 1 presents the mean results of the equal error rate for all 50 users for several stroke sequence lengths. As shown, the mean value and the standard deviation of the EER progressively decrease as more strokes are added to the decision rule. In Figure 6 we present Receiver Operating Characteristic (ROC) curves for the case of 10 and 15 digit PINs, corresponding to EER of 12.5% (10 digits) and 6.2% (15 digits).

4.1. On Guessing Entropy

We describe an information theoretic measure to evaluate the contribution of a biometric characteristic in a conventional password/PIN authentication system. We describe the Guessing Entropy [12][13] measure in a general situation and apply it to our particular case of using a PIN code combined with mouse movement behavior.

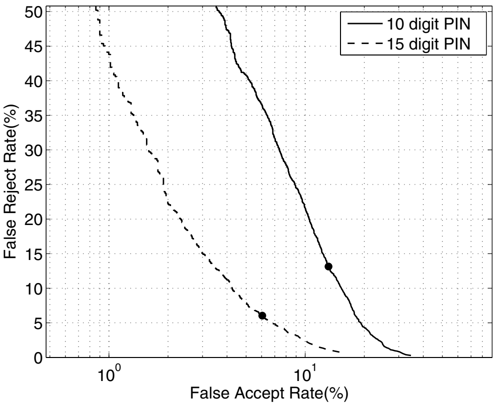

Fig. 6. ROC curves for the mouse movement biometric for two different lengths of the PIN code. Dots mark the EER: 12.5% for 10 digit PIN, 6.2% for 15 digit PIN.

Shannon defined the entropy [14] in the context of Information Theory as the average information content in a message. The entropy of a message (in bits) is given by Eq. (2), where x is an event with probability $p(x)$.

$$H(x) = -\sum_{x} p(x) log_2(p(x)). \tag{2}$$

In the case of a randomly generated password composed of l characters from a set with size b, the Shannon entropy is simplified to Eq. (3), called the Guessing Entropy; it is the number of tries needed to guess a password. We will use the bit unit to measure the Guessing Entropy.

$$GH(pass) = log_2(b^l). \tag{3}$$

Equation (3) is applicable for cases where the password is chosen randomly. In typical cases, where the user selects his own (non-random) password, entropy in Eq. (3) decreases given that the characters of the password are not independent.

The NIST e-Authentication guidelines [15] provide the following estimates of Guessing Entropy for user-selected digit PIN codes: first digit - 3 bits; next 4 digits - 2 bits per digit, 6th digit and above - 1 bit per digit.

Consider a biometric system that is operating at a particular value of False Acceptance Rate (FAR_o) and False Rejection Rate (FRR_o). We consider this biometric system comparable to a password based system with $\left\lceil \frac{1}{FAR_o} \right\rceil$ possible codes, where $\lceil a \rceil$ is the *ceil* operation. Given that on some occasions the system rejects a legitimate user (with FRR_o probability), it is assumed that the system will permit the user to retry, reducing the Guessing Entropy of the biometric method by $log_2(N_{tries})$. The overall Guessing Entropy is expressed in Eq. (4).

$$GH = \log_2 \left\lceil \frac{1}{FAR_o} \right\rceil - \log_2(N_{tries}). \tag{4}$$

To select a number of tries we can establish a Total Rejection Ratio (TRR_o) corresponding to the probability of the system blocking the access to an user. We will assume that all the tries are independent and that the combined rejection rate is the power of the base FRR_o to the number of tries. From this assumption we compute the number of tries needed to guarantee a particular TRR_o given the FRR of the biometric system (see Eq. (5)).

$$\begin{aligned} FRR_o^{N_{tries}} &< TRR_o. \\ N_{tries} &= \left\lceil \frac{log(TRR_o)}{log(FRR_o)}. \right\rceil . \end{aligned} \tag{5}$$

In our system we determined the effect of the length of the PIN code on Guessing Entropy in three cases: 1) PIN code alone; 2) mouse movement alone; 3) combination of PIN and mouse movement. Establishing a Total Rejection Ratio to be less than 1%, the system has to grant 2 attempts given the FRR_o of the mouse movement biometric technique. The entropy of a PIN code increases with the length of the PIN code.

E-Authentication systems have been classified into 4 levels [15], expressing the degree of certainty in the user identity. Level 1 is the lowest assurance and level 4 is the highest. The first two levels can be implemented via passwords, where the requirements for the password entropy are $H(code) > 10$ (requiring 1,024 attempts) for level 1 and $H(code) > 14$ (requiring 16,384 attempts) for level 2.

Figure 7 shows the relationship between the length of the PIN code and the entropy for the three authentication methods described above. For the required entropy for level 1 security (10 bits or 6 digit PIN), the introduction of the mouse movement biometric reduces the need to memorize two of the six digits (needing only a 4 digit PIN). The same observation is true for level 2 requirements, where 14 bits correspond to a 10 digit PIN when alone or to a 8 digit PIN when the mouse movement biometric is introduced. Alternatively, use of mouse movement along with the PIN code increases the Guessing Entropy equivalent to append 2 digits to the PIN code.

5. DISCUSSION

We have presented a new soft biometric technique implemented in a web-based environment that improves security in login applications. The system records the mouse movement of the user while he inserts his user name and PIN code. The overall security level can be designed to meet standard security levels with smaller PIN codes compared to a PIN code only based solution. We also note that depending on the length of the PIN code, the WebBiometrics system decreases the verification error of the biometric technique.

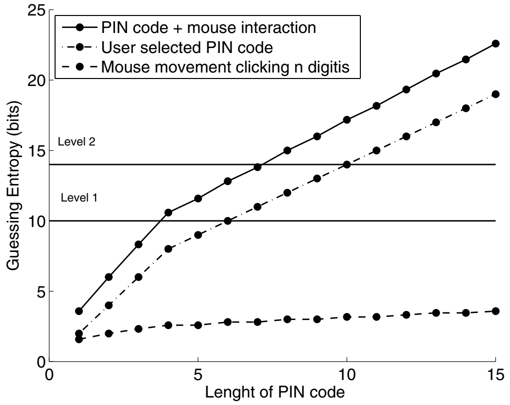

Fig. 7. The Guessing Entropy of (i) mouse movement biometric (ii) PIN code (iii) combination of mouse movement biometric and PIN code.

Table 2 compares some other behavioral biometric techniques with the proposed mouse movement biometric with different strokes length durations. Given the performance of the proposed biometric technique, when used for short strokes lengths as is typical in a login step, it can only be considered as a soft biometric [16].

5.1. Advantages

The proposed system does not modify the normal login process of a conventional on-line security system. There is only a software modification of the server login protocol, providing an incremental security layer that is difficult to circumvent even if the user willingly provides access to someone else. Although PIN code can be given or stolen easily, the interaction behavior is very difficult to mimic.

5.2. Problems

This implementation introduces some usability issues, given that persons with disabilities that can not use the mouse, do not present this biometric trait. It is also possible that some users have characteristics that will produce interaction behavior that can not be measured by our system. We have not addressed this problem of the quality of user interaction to filter some of the users. In our study all the 50 users whose data was available were used in the performance values reported. Our study currently requires that the user always uses the same computer with the same mouse.

5.3. Future work

We plan to collect user mouse movements data on different mouse/computer and determine the on the performance of the

Table 2. A Comparison of various behavioral biometric techniques.

Technique	EER	Pros	Cons
Voice Dynamics [4]	$\sim 5\%$	easy to collect	Sensitive to noise and voice alterations
Keystroke Dynamics [5]	$\sim 4\%$	non-intrusive method	keystrokes can be replayed
Signature Dynamics [3]	$\sim 2\%$	difficult to reproduce	requires additional hardware
Mouse Movement		simple addon to other security systems, low intrusion and hard to reproduce	poor performance for short interaction periods
10 strokes	$\sim 10\%$		
20 strokes	$\sim 5\%$		
30 strokes	$\sim 2\%$		

system.

The mouse movements biometric trait needs an extensive validation in a implementation scenario, conduced by an industry partner that would provide a bigger population and the requirements for a deployment solution.

6. REFERENCES

[1] Anurag Acharya, Matt Cutts, Jeffrey Dean, Paul Haahr, and Monika Henzinger, "USPSN 748664 - information retrieval based on historical data," United States Patent and Trademark Office, December 2003.

[2] "Behavioral targeting," 2005, Accessed on April 19, 2007: http://advertising.yahoo.com/marketing/bt/.

[3] Jonghyon Yi, Chulhan Lee, and Jaihie Kim, "Online signature verification using temporal shift estimated by the phase of gabor filter," *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 776– 783, 2005.

[4] Daniel Ramos-Castro, Julian Fierrez-Aguilar, Joaquin Gonzalez-Rodriguez, and Javier Ortega-Garcia, "Speaker verification using speaker- and test-dependent fast score normalization," *Pattern Recogn. Lett.*, vol. 28, no. 1, pp. 90–98, 2007.

[5] Fabian Monrose and Aviel D. Rubin, "Keystroke dynamics as a biometric for authentication," *Future Generation Computer Systems*, vol. 16, no. 4, 2000.

[6] Luis von Ahn, Manuel Blum, and John Langford, "Telling humans and computers apart automatically," *Communications of the ACM*, vol. 47(2), pp. 56–60, 2004.

[7] Hugo Gamboa and Ana Fred, "A behavioral biometric system based on human-computer interaction," in *SPIE 5404 - Biometric Technology for Human Identification*, A. K. Jain and N. K. Ratha, Eds., Orlando, USA, August 2004, pp. 381–392.

[8] Hugo Gamboa and Vasco Ferreira, "Widam - web interaction display and monitoring," in *5th International Conference on Enterprise Information Systems, ICEIS'2003*, Anger, France, 2003, pp. 21–27, INSTICC Press.

[9] Arnaud Le Hors, Philippe Le Hgaret, and Lauren Wood, "Document object model level 2 core," Tech. Rep., World Wide Web Consortium (W3C), 2000.

[10] Anil K. Jain, Robert P. W. Duin, and Jianchang Mao, "Statistical pattern recognition: A review," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 1, pp. 4–37, 2000.

[11] Bradley Efron and Robert J. Tibshirani, *An Introduction to the Bootstrap*, Chapman & Hall, 1993.

[12] James L. Massey, "Guessing and entropy," in *IEEE International Symposium on Information Theory*, Trondheim, Norway, 1994, p. 204.

[13] Christian Cachin, *Entropy Measures and Unconditional Security in Cryptography*, Ph.D. thesis, Swiss Federal Institute of Technology Zurich, 1997.

[14] Claude E. Shannon, "A mathematical theory of communication," *Bell Systems Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948, Continued 27(4):623-656.

[15] William E. Burr, Donna F. Dodson, and W. Timothy Polk, "NIST special publication 800-63 electronic authentication guideline," Tech. Rep., National Institute of Standards and Technology, April 2006.

[16] A. K. Jain, S. C. Dass, and K. Nandakumar, "Can soft biometric traits assist user recognition?," in *Biometric Technology for Human Identification. Edited by Jain, Anil K.; Ratha, Nalini K. Proceedings of the SPIE, Volume 5404, pp. 561-572 (2004).*, A. K. Jain and N. K. Ratha, Eds., Aug. 2004, vol. 5404 of *Presented at the Society of Photo-Optical Instrumentation Engineers (SPIE) Conference*, pp. 561–572.