Signature Verification Based on Moments Technique

Shaymaa S. M. Al-Juboori
Dept. of Computer Sci./College of Education for Pure Science(Ibn Al-Haitham) / University of Baghdad

Received in : 29April 2013, Accepted in : 19 May 2013

Abstract
In this research we will present the signature as a key to the biometric authentication technique. I shall use moment invariants as a tool to make a decision about any signature which is belonging to the certain person or not. Eighteen voluntaries give 108 signatures as a sample to test the proposed system, six samples belong to each person were taken. Moment invariants are used to build a feature vector stored in this system. Euclidean distance measure used to compute the distance between the specific signatures of persons saved in this system and with new sample acquired to same persons for making decision about the new signature. Each signature is acquired by scanner in jpg format with 300DPI. Matlab used to implement this system.

Keywords: Signature, Biometric, Euclidean Distance, Binary Image, Verification, Image Enhancement, Canny Edge Detection, Median Filter.

Introduction

Information security is concerned with the assurance of confidentiality, integrity and availability of information in all forms. There are many tools and techniques that can support the management of information security. But system based on biometric has been evolved to support some aspects of information security. Biometric authentication supports the facet of identification, authentication and non-repudiation in information security [1]. A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. Biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics [2]. Security is "the quality or state of being secured to be free from danger.". In other words, protection against adversaries—from those who would do harm, intentionally or otherwise—is the objective. National security, for example, is a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people. Achieving the appropriate level of security for an organization also requires a multifaceted system. A successful organization should have the following multiple layers of security in place to protect its operations:

- **Physical security**, to protect physical items, objects, or areas from unauthorized access and misuse.
- **Personnel security**, to protect the individual or group of individuals who are authorized to access the organization and its operations.
- **Operations security**, to protect the details of a particular operation or series of activities.
- **Communications security**, to protect communications media, technology, and content.
- **Network security**, to protect networking components, connections, and contents.
- **Information security**, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission [3].

The security requirements of the today's society have placed biometrics at the center of a large debate, as it is becoming a key aspect in a multitude of applications. What biological measurements are qualified to be a biometric?

Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- Universality: each person should have the characteristic.
- Distinctiveness: any two persons should be sufficiently different in terms of the characteristic.
- Permanence: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
- Collectability: the characteristic can be measured quantitatively [4].

Biometrics

Biometrics is the analysis of biological observations and phenomena. People routinely use biometrics to recognize other people, commonly using the shape of a face or the sound of a voice to do so. Biometrics can also be used to create automated ways of recognizing a person based on her physiological or behavioral characteristics. Using biometrics as the basis of technologies that can be used to recognize people [5]. A biometric system is essentially a pattern recognition system that makes use of biometric traits to recognize individuals. The objective is to establish an identity based on 'who you are or what you produce', rather than by 'what you possess' or 'what you know'. The significance of using biometrics has been reinforced by the need for large scale identity management systems. The very purpose of identity management is to accurately determine an individual‘s identity in the context of

several different applications. This new technique not only provides enhanced security but also avoids, in authentication the need to remember several passwords and maintain multiple authentication tokens [6]. Biometrics systems can be used as a means of authenticating a user. When they are used in this way, a user presents his biometric data along with his identity, and the biometric system decides whether or not the biometric data presented is correct for that identity. Biometrics used as a method of authentication can be very useful, but authentication systems based on biometrics also have very different properties from other authentication technologies, and these differences should be understood before biometrics are used as part of an information security system. Systems based on biometrics can also be used as a means of identification. When they are used in this way, captured biometric data is compared to entries in a database, and the biometric system determines whether or not, the biometric data presented matches any of these existing entries. When biometrics are used for identification, they have a property that many other identification systems do not have. In particular, biometrics do not always require the active participation of a subject [5]. On-line verification must be differentiated from off-line verification, as the number of features, which may be extracted from on-line mediums, surpass those obtained from off-line verification i.e. time, pressure and velocity can be extracted from on-line modes of verification [7].

Biometric System

All biometric systems consist of three basic elements:

- Enrollment or the process of collecting biometric samples from an individual, known as the enrollee, and the subsequent generation of template.
- Templates, or the data representing the enrollee‘s biometric.
- Matching, or the process of comparing a live biometric sample against one or many templates in the system database [6].

Biometric system refers to the various individual components (like sensors, matching algorithm, and result display) that combine to make an operational biometric system.

A biometric system is an automated system capable of:

1. Capturing a biometric sample from an end user
2. Extracting and processing the biometric data from that sample
3. Storing the extracted information in a database
4. Comparing the biometric data with data contained in one or more reference references
5. Deciding how well they match and indicating whether or not an identification or verification of identity has been achieved [8].

Biometric Technologies

The function of a biometric technologies authentication system is to facilitate controlled access to applications, networks, personal computers (PCs), and physical facilities. A biometric authentication system is essentially a method of establishing a person‘s identity by comparing the binary code of a uniquely specific biological or physical characteristic to the binary code of an electronically stored characteristic called a biometric. The various biometric technologies are DNA, Ear, Face, Facial thermogram, Fingerprint, Gait, Hand geometry, Hand Vein, Iris, Keystroke, Odor, Retina, Signature, Voice and Palmprint [6]. Human signature represents some of the most common biometric patterns that our visual system encounters daily [5]. Signature is an important biometric measure, which are subject to intrapersonal variation. An automated system for signature verification is feasible only if the representation of the signature image is insensitive to intra-personal variations, but sensitive to inter-personal variations. The goal is to maximize the distance between signatures of different individuals, the maximizing constraint being that the distance between the signatures of the same person is kept constant or minimized [9].

Signature Verification Technique

A signature recognition and verification system is a system capable of efficiently addressing two individuals but strongly related tasks: (a) identification of the signature owner and, (b) decision whether the signature is genuine or forger. Within the field of human classification, the procedure of biometrics is emergent because of its distinctive properties [7].

The signature dynamics recognition is based on the dynamics of making the signature, rather than a direct comparison of the signature itself afterwards. The dynamics is measured as a means of the pressure, direction, acceleration and the length of the strokes, dynamics number of strokes and their duration. The most obvious and important advantage of this is that a fraudster cannot glean any information on how to write the signature by simply looking at one that has been previously written [1]**.** The way a person signs his or her name is known to be a characteristic of that individual. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of verification. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary substantially: even successive impressions of their signature are significantly different. Further, professional forgers may be able to reproduce signatures that fool the system [4].

Types of Signature Verification

Based on the definitions of signature, it can lead to two different approaches of signature verification.

1- Off-Line or Static Signature Verification Technique: This approach is based on static characteristics of the signature which are invariant. In this sense signature verification, becomes a typical pattern recognition task knowing that variations in signature pattern are inevitable; the task of signature authentication can be narrowed to drawing the threshold of the range of genuine variation. In the offline signature verification techniques, images of the signatures written on a paper are obtained using a scanner or a camera.

2- On-line or Dynamic Signature Verification Technique: This is the second type of signature verification technique. This approach is based on dynamic characteristics of the process of signing. This verification uses signatures that are captured by pressure sensitive tablets that extract dynamic properties of a signature in addition to its shape. Dynamic features include the number of order of the strokes, the overall speed of the signature and the pen pressure at each point that makes the signature more unique and more difficult to forge [10].

Online signature verification is based on dynamic features of the signature extracted as the signature is being signed. It is a process that is more resilient to forgery than offline signature verification since the process is not directly visible to man but machine [11].

Hu's invariant moments

The general form of a regular moment function m_{pq} of order $(p + q)$ of an image intensity function $f(x, y)$ can be given as,

$$m_{pq} = \iint x^p y^q f(x, y)\mathrm{d}x\mathrm{d}y$$

For a digital image, the central moments, which are invariant to translation, are defined as:

$$\mu_{pq} = \sum_x \sum_y (x - xc)^p (y - yc)^p f(x, y)$$

Where, $xc = m10/m00$ and $yc = m01/m00$ are the co-ordinates of the centroid [12].

The seven Hu invariants moments are calculated by:

$$\varphi_1 = \eta_{20} + \eta_{02}, \quad \varphi_2 = (\eta_{20} - \eta_{02})^2 + 4\eta_{11}$$
$$\varphi_3 = (\eta_{30} - 3\eta_{12})^2 + (3\eta_{21} - \eta_{03})^2$$
$$\varphi_4 = (\eta_{30} + \eta_{12})^2 + (\eta_{03} + \eta_{21})^2$$
$$\varphi_5 = (\eta_{30} - 3\eta_{12})(\eta_{30} + \eta_{12})\left[(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2\right] + (3\eta_{21} - \eta_{03})(\eta_{21} + \eta_{03})\left[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2\right]$$
$$\varphi_6 = (\eta_{20} - \eta_{02})\left[(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2\right] + 4\eta_{11}(\eta_{30} + \eta_{12})(\eta_{21} + \eta_{03})$$
$$\varphi_7 = (3\eta_{21} - \eta_{03})(\eta_{30} + \eta_{12})\left[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2\right] - (\eta_{30} - 3\eta_{12})(\eta_{03} + \eta_{12})\left[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2\right]$$

These Hu's seven invariant moments are invariant under translation, rotation and scaling. Some pattern recognition applications such as hand printed characters, aircraft identification and ship recognition have included [13].

Binary Image

The pixels in a binary image can assume only two values, 0 or 1; a gray image may be quantized to a number of intensity levels, depending on the application, while a color image may be quantized in different color bands. As the number of intensity levels increases, the image is represented to a better approximation, although the storage requirements also grow proportionately. The binary images are thus least expensive, since the storage and also processing requirement is the least in case of binary images. Examples of binary images are line drawings, printed text on a white page, or silhouette. These images contain enough information about the objects in the image and we can recognize them easily. There are a number of applications in computer vision where binary images are used for object recognition, tracking, and so on. The applicability of binary images is, however, limited because the overall information content in such images is limited. A gray level image maybe converted into a binary image by thresholding process [9].

Image Enhancement

The purpose of image enhancement is to improve the visual appearance of an image, or to transform an image into a form that is better suited for human interpretation or machine analysis. Although there exists a multitude of image enhancement techniques, surprisingly, there does not exist a corresponding unifying theory of image enhancement. This is due to the absence of a general standard of image quality that could serve as a design criterion for image enhancement algorithms [14]. Image enhancement is among the simplest and most appealing areas of digital image processing. Basically, the idea behind enhancement techniques is to bring out detail that is obscured, or simply to highlight certain features of interest in an image[15].

Median Filter

Median filtering is a nonlinear signal processing technique developed by Tukey that is useful for noise suppression in images. In one-dimensional form, the median filter consists of a sliding window encompassing an odd number of pixels. The center pixel in the window is replaced by the median of the pixels in the window. The median of a discrete sequence a1, a2,..., aN for N odd is that member of the sequence for which (N – 1)/2 elements are smaller or equal in value and (N – 1)/2 elements are larger or equal in value. The concept of the median filter can be extended easily into two dimensions by utilizing a two-dimensional window of some desired shape such as a rectangle or discrete approximation to a circle. It is

obvious that a two-dimensional median filter will provide a greater degree of noise suppression than sequential processing with median filters, but two-dimensional processing also results in greater signal suppression [16]. A special type of low-pass filter is the median filter. The median filter takes an area of an image (3x3, 5x5, 7x7, etc.), looks at all the pixel values in that area, and replaces the center pixel with the median value. The median filter does not require convolution. It does, however, require sorting the values in the image area to find the median value. There are two noteworthy features of the median filter. First, it is easy to change the size of the median filter. (The images later will show the effect of using a different size.) Implementing the different size is a simple matter of for loops in the code. Second, median filters remove noise in images, but change noise-free parts of images minimally [17].

The Canny Edge Detector

The Canny edge detector is widely considered to be the standard edge detection algorithm in the industry. It was first created by John Canny for his Masters thesis at MIT in 1983, and still outperforms many of the newer algorithms that have been developed. Canny saw the edge detection problem as a signal processing optimization problem, so he developed an objective function to be optimized. The solution to this problem was a rather complex exponential function, but Canny found several ways to approximate and optimize the edge-searching problem. The steps in the Canny edge detector are as follows:

1. Smooth the image with a two dimensional Gaussian. In most cases the computation of a two dimensional Gaussian is costly, so it is approximated by two one dimensional Gaussians, one in the x direction and the other in the y direction.
2. Take the gradient of the image. This shows changes in intensity, which indicates the presence of edges. This actually gives two results, the gradient in the x direction and the gradient in the y direction. ..... (4)
3. Non-maximal suppression. Edges will occur at points the where the gradient is at a maximum. Therefore, all points not at a maximum should be suppressed. In order to do this, the magnitude and direction of the gradient is computed at each pixel. Then for each pixel check if the magnitude of the gradient is greater at one pixel's distance away in either the positive or the negative direction perpendicular to the gradient. If the pixel is not greater than both, suppress it.
4. Edge Thresholding. The method of thresholding used by the Canny Edge Detector is referred to as "hysteresis". It makes use of both a high threshold and a low threshold. If a pixel has a value above the high threshold, it is set as an edge pixel. If a pixel has a value above the low threshold and is the neighbor of an edge pixel, it is set as an edge pixel as well. If a pixel has a value above the low threshold but is not the neighbor of an edge pixel, it is not set as an edge pixel. If a pixel has a value below the low threshold, it is never set as an edge pixel [18].

The Canny edge detector arises from the earlier work of Marr and Hildreth, who were concerned with modeling the early stages of human visual perception. In designing his edge detector he concentrated an ideal step edge, represented as a Sign function in one dimension, corrupted by an assumed Gaussian noise process. In practice, this is not an exact model but it represents an approximation to the effects of sensor noise, sampling and quantisation. The approach was based strongly on convolution of the image function with Gaussian operators and their derivatives, so we shall consider these initially.

Considering the Gaussian function in one dimension, this may be expressed

$$G(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{-x^2}{2\sigma^2}}$$

And the first derivative is

$$G'(x) = \frac{\dots}{\sqrt{2\pi}\sigma^3} e^{\frac{-x^2}{2\sigma^2}} \quad (10)$$

And the second derivative is

$$G''(x) = -\frac{1}{\sqrt{2\pi}\sigma^3} e^{\frac{-x^2}{2\sigma^2}} \left[1 - \frac{x^2}{\sigma^2}\right]$$

The equivalent 2D functions are most easily expressed with respect to a polar

$$r = sqrtx^2 + y^2 \quad \dots\dots\dots\dots \quad (11)$$

Coordinate system where represents the radial distance from the origin. The function is symmetrical and independent of θ. Thus,

$$G(r) = \frac{1}{2\pi\sigma^2} e^{\frac{-r^2}{2\sigma^2}} \quad \dots\dots\dots\dots \quad (12)$$

And the first derivative is,

$$G'(r) = \frac{-r}{2\pi\sigma^4} e^{\frac{-r^2}{2\sigma^2}}$$

And the second derivative is,

$$G''(x) = -\frac{1}{2\pi\sigma^4} e^{\frac{-r^2}{2\sigma^2}} \left[1 - \frac{r^2}{\sigma^2}\right] \dots\dots\dots\dots \quad (13)$$

Now consider an ideal step edge. When convolved with a Gaussian function. The next sketches show the first and second derivatives; the presence and location of the edge is marked by a peak and a zero crossing respectively.
In fact, the first derivative of the image function convolved with a Gaussian,

$$g(x, y) = D[Gauss(x, y) * f(x, y)]$$

Is equivalent to the image function convolved with the first derivative of a Gaussian,

$$g(x, y) = D[Gauss(x, y)] * f(x, y) \quad \dots\dots\dots\dots \quad (5)$$

Therefore, it is possible to combine the smoothing and detection stages into a single convolution in one dimension, either convolving with the first derivative of the Gaussian and looking for peaks, or with the second derivative and looking for zero crossings [19].

..... (6)

Euclidean distance

The Euclidean distance of (υ_1, ζ_1) and (υ_2, ζ_2)

$\sqrt{\Delta\xi^2 + \Delta u^2}$

, $\Delta\upsilon=\upsilon_2-\upsilon_1$, $\Delta\zeta = \zeta_2- \zeta_1$ [20] ..... (7)

The Proposed Signature Verification Algorithm

In this section, I will present many steps that summarize the proposed signature verification algorithm:

1- Acquire the five samples signature to each voluntary in jpg format, 300 DPI.

2- Enhance the acquired signature image by applying median filter to remove noise suppression from the signature. ..... (8)

3- Applying canny edge detector on the signature image to detect the signature edges.

4- Convert the target signature image to binary image by using the global threshold value for the image.

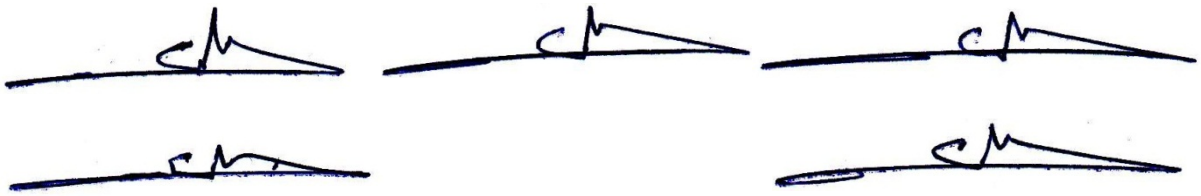
5- The seven Hu invariants moments for each voluntary (5 samples of signatures) are ..... (9) calculated and used to compute the standard deviation for the average of moments belongs to

each voluntary and saved as a feature vector. The sample order 6 is used for verification operation.
The above steps will be repeated to all samples (18 persons and 5 samples to each person).
After that, the proposed system is ready to verify any certain person by comparing the feature vector belong to him that saved in this system with the feature vector that is excluded from his exact signature (do the previous steps 1-5 to his exact signature). The comparing process is achieved by computing the Euclidian distances between the saved and the new feature vector.

The following section shows the applying steps from (1 to 5) to demonstrate the result for the proposed system.

Experimental Results

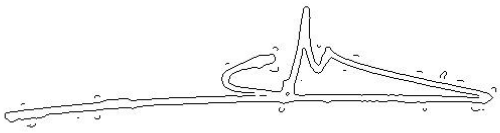
1- Acquired the signatures to all voluntaries, the following signatures are belong to person1.



2- Signature order 1after applying median filter on it.

3- Signature order 1 after applying canny edge detector on it.

4- The binary image resulting from the previous step is.



5- The seven Hu invariants moments for the above signature in step 4 is explained in table 1.

Conclusions

The decision about acceptance or rejection of any tested signature will depend on the distance between the saved and computed standard deviation, if the result between the minimum and the maximum means acceptance. The proposed system may be used in online or offline mode applications. The accuracy of the results depends on the quality and resolution of the samples. The number of samples for each person is a big factor that affects in the truth of results. Preprocessing to the acquired samples that play basic role in making decision about the result

of verification. The samples of each person must be acquired in different times, not in the same time to assure this sample is variance.

References

1- Debnath, Bhattacharyya; Rahul, Ranjan; Farkhod, Alisherov A; and Minkyu Choi, (2009) "Biometric Authentication: A Review", International Journal of u- and e- Service, Science and Technology, 2(3):1-8.
2- Anil, K. Jain; Arun Ross and Salil Prabhakar, (2004), An Introduction to Biometric Recognition", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, 14:(1).
3- Michael, E.; Whitman and Herbert J.; Mattord (2012) Principles of Information Security" Fourth Edition, Cengage Learning Customer & Sales Support, USA.
4- Anil, K. Jain; Arun, Ross, and Salil Prabhakar (2004) ,An Introduction to Biometric Recognition", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, 14:1:4.
5- John, Vacca (2009) ,References Computer and Information Security Handbook, Elsevier, USA.
6- Asha , S.and Chellappan C. (February 2012) ,Biometrics: An Overview of the Technology, Issues and Applications, International Journal of Computer Applications (0975 – 8887) 39(1):1,3,4.
7- Vibha, Pandey and Sanjivani Shantaiya (2012), "A Novel Approach for Signature Verification using Artificial Neural Network", International Journal of Engineering and Advanced Technology (IJEAT) , Vol. 1, Issue-6:163.
8- http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=74
9- Tinku, Acharya and Ajoy K. Ray ,(2005),"Image Processing Principles and Applications", JOHN WILEY & SONS,USA.
10- Sachin, A. Murab and Vaishali. M.Deshmukh, (2012), "An Empirical Study of Signature Recognition &Verification System Using Various Approaches", International Journal of Engineering and Advanced Technology (IJEAT), Volume 2, Issue-2:260.
11- Ibiyemi, T.S, Ogunsakin J. and Daramola S.A, (2012), "Bi-Modal Biometric Authentication by Face Recognition and Signature Verification", International Journal of Computer Applications (0975 – 8887) Vol. 42, No. 20:17.
12- KUNTE R SANJEEV and SUDHAKER R D SAMUEL (2007) "A simple and efficient optical character recognition system for basic symbols in printed Kannada text", Sadhana Vol. 32, Part 5:254.
13- Derya, Avci and Asaf, Varol (2009) "An expert diagnosis system for classification of human parasite eggs based on multi-class SVM" , Expert Systems with Applications 36:45
14- Gerhard, X. Ritter and Joseph, N. Wilson, (2001), "Handbook of computer vision algorithms in image algebra", Second Edition, CRC Press, USA.
15- Rafael, C. Gonzalez and Richard, E. Woods(2002) "Digital Image Processing", Second Edition, Prentice Hall, USA.
16- William K. Pratt, (2001),"Digital Image Processing",John Wiley & Sons, Third Edition,USA
17- Dwayne, Phillips (2000) "Image Processing in C",Second Edition, R & D Publications, USA
18- Ehsan, Nadernejad (2008) "Edge Detection Techniques: Evaluations and Comparisons, Applied Mathematical Sciences", Vol. 2, , No. 31: 1507 – 1520.
19-http://homepages.inf.ed.ac.uk/rbf/CVonline/LOCAL_COPIES/MARBLE/low/edges/canny.htm
20-Stéphane, Mallat (1999) "A Wavelet Tour of Signal Processing", Second Edition, Academic Press, USA

Table 1: Shows seven Hu invariants moments for the signature of pereon1

Moment No.	Moment Values
1	2.26711242134623390e+004
2	3.96714646405897260e+008
3	4.78969441748034860e+006
4	2.69812883371203590e+003
5	4.19073083574773200e+013
6	1.40389948470549800e+011
7	-9.12176428165768750e+012

Table 2: Shows the standard deviations to all samples used to apply the proposed system

Sample No.	Minimum Standard Deviation	Maximum Standard Deviation
1	2.9492697067217676e+012	4.2704646689106398e+013
2	1.6513198590601340e+011	3.1037919790873461e+013
3	7.5168839043572083e+009	3.5701857629788091e+012
4	2.5585349949207005e+010	6.6297830558730312e+014
5	6.1289991889752344e+011	1.2212215513994287e+015
6	2.2881853796696342e+010	2.4644980505726889e+011
7	3.5302934094661023e+011	5.9228561232047250e+014
8	8.5487006945504922e+013	2.3675039145631285e+015
9	5.4434987969066748e+012	6.2696768091142325e+014
10	4.4922111292388848e+012	6.4831158571791891e+013
11	1.1065455107767971e+012	2.3506293785080664e+013
12	6.8355516830620542e+007	4.0768717744245079e+010
13	2.7260952959002689e+011	2.1088337836302234e+014
14	1.5587438142523291e+010	1.4287765417277476e+012
15	6.8546564999533529e+009	4.2060508646639897e+012
16	4.4142298477591076e+009	4.5465624178469658e+010
17	2.3362028685872781e+013	2.0866690567886756e+014
18	4.2859539992639148e+008	1.8163972505661336e+013

التحقق من التوقيع بالاعتماد على التغير اللحظي

شيماء شاكرمحمود الجبوري
قسم علوم الحاسبات / كلية التربية للعلوم الصرفة (ابن الهيثم) / جامعة بغداد

الخلاصة
في هذ البحث سوف نعرض التوقيع مفتاحا للتحقق الى تقانة الإحصاء البايولوجي. وسنستخدم تقانة التغير اللحظي أداةً لأتخاذ القرار حول أي توقيع هل يعود إلى شخص معين أم لا؟ ثمانية عشرمتطوعا مع 108 توقيع أخذتها عينة لاختبار النظام المقترح، ست عينات إلى كل شخص. التغير اللحظي اسستخدم لبناء متجه الصفات المخزونة في هذا النظام. مقياس اقليدس للمسافة استخدم لحساب المسافة بين التوقيعات المحددة للأشخاص المخزونة في هذا النظام مع العينة الجديدة المكتسبة إلى الأشخاص أنفسهم لغرض اتخاذ القرارحول عائدية التوقيع الجديد. كل التواقيع تم الحصول علىها باستخدام الماسح الضوئي بصيغة (jpg format, 300DPI) ، استخدام الماتلاب لغرض تنفيذ النظام المقترح.

الكلمات المفتاحية: التوقيع ، الاحصاء البايولوجي ، الصورة الثنائية، التحقق، تحسين الصورة، كاني لتحديد الحواف، مرشح المتوسط.