A Hybrid Algorithm to Protect Computer Networks Based on Human Biometrics and Computer Attributes

Rahim Abdul-Al Sahib Ogla
Dept. of Computer Science/ University of Technology/ Baghdad

Received in:26/January/2016,Accepted in:3/October/2016

Abstract

Objective of this work is the mixing between human biometric characteristics and unique attributes of the computer in order to protect computer networks and resources environments through the development of authentication and authorization techniques. In human biometric side has been studying the best methods and algorithms used, and the conclusion is that the fingerprint is the best, but it has some flaws. Fingerprint algorithm has been improved so that their performance can be adapted to enhance the clarity of the edge of the gully structures of pictures fingerprint, taking into account the evaluation of the direction of the nearby edges and repeat.

In the side of the computer features, computer and its components like human have unique characteristics. A program has been produced in the Visual Basic environment. The goal of this program is to get the computer characteristics and merge them with human characteristics to produce powerful algorithms of authentication and authorization can be used to protect the resources that are stored in the computer networks environments through the creation of software modules and interactive interfaces to accomplish this purpose.

Keywords: Biometrics, Biometrics features, Authentication, Authorization, Security ,Computer Attributes ,Encryption / Decryption, fingerprints

Introduction

The verification has dependable approval turned into a basic piece of each man's lifetime for various routine implementations. The computerized of biometrics are a good strategy for perceiving a user taking into account a behavioral and/or physiological trademark. However, the biometrics in its early frame have various tractable perspectives like security, system recovery, and data integrity and fault tolerance. The reliable solution is viewed to secure the personality and the privileges of people such as perceiving remarkable and permanent components. The usefulness of biometrics is utilized for two authentication methods which are illustrated with Figure(1).

- **The identification** includes building up a man's character construct just with respect to biometric estimations. The comparator matches the obtain biometric with the ones put away in the database bank utilizing from $1 \rightarrow N$ matching according to the algorithm of identification that can be found in [1] ,[2] and [3].
- **The Authentication** includes affirming or rejecting the user's claimed identity. The identifier of man (e.g. ID number) is a basic identity acknowledged and a biometric format is taken to a coordinated utilizing from $1 \rightarrow 1$ matching depend on algorithm to affirm the individual's identity [3]. The legitimacy of a biometric framework can't be premeditated precisely, which must be specified in the case of slips similar to the possibility of tolerating a gatecrasher.

In suggested work, the biometric data and computer attributes is combining to produce hybrid robust algorithm, the security components are improved. The following sections show the methodology of the proposed mixing between the biometric data and the computer which attributes to secure computer network and its resources. [11] and [12].

Classifications of Biometrics

Some biometrics are used as a feature of humans that can be classifies as shown in table (1). [7]. Biometrics is fundamentally the acknowledgment of human qualities that are exceptional to every human, which can incorporate DNA, facial recognition, retina outputs, voice recognition, fingerprints, palm prints, etc. as shown in table(1). Some public metrology, which can be used to determine the characteristics of biological humans possible inclusion in table (2) adopt and integrate them with the characteristics of computer to get a new hybrid algorithm for securing computer networks and their sources.[8]and [13].

Biometric Devices Types

Some of these devices (Table (3**)**) have been used in our work in order to achieve adequate protection for networks and their sources (data, applications) to prevent unauthorized person from penetrating networks and access to the database stored within the servers or those transferred through networks media. [2],[4] and [6].

Fingerprint Authentication

The investigation into fingerprints for coordinating purposes of the most part needs the comparison of a few components of the print patterns. These contain patterns, which are total qualities of ridges, and minutia points, which are interesting elements found inside of the patterns. In addition, the importance of analyzing the structure and properties of human leather are keeping in mind the result is into effectively utilizing a portion of the imaging advancements. Three essential patterns are fingerprint buttresses can be stated in the loop, Arch and whorl:

- **Loop:** The finger is entering direct with the edges, also framework a curve, and end process for exit.
- **Arch:** The edges enters from one side of the finger, ascend in the inside framing a circular segment, and afterward leave the opposite side of the finger.
- **Whorl:** Ridges frame circularly around a main issue on the finger [13]and [14].

Researchers have found that relatives frequently have the same general fingerprint patterns, prompting the conviction that these patterns are acquired as Shown in Figure (2).

Fingerprints Via Iris recognition

The proposed work focuses on avoiding weaknesses in the fingerprint ,So, hybrid algorithm is created to combine human characteristics and the characteristics of the computer in order to find an algorithm that provides strong protection of sources networks. Here are some of the weaknesses in fingerprints compared with iris recognition. [4] and [15]

- Fingerprint false accept rate varies by vendor, and is approximately 1 in 100,000. Iris recognition false accept rate is 1 in 1.2 million statistically..
- Most high-end fingerprint systems measure approximately 40-60 characteristics; while iris recognition looks at about 240 characteristics to create the unique Iris Code
- Fingerprint searches take much longer, may require filtering, and may return multiple candidate matches.
- The long association of fingerprints with criminals makes this biometric an uncomfortable method of authentication for some people.
- Most systems require physical contact with a scanner device that needs to be kept clean (hygiene issue).
- Based on occupation, trauma or disease, individual fingerprints may be obscured, damaged or changed — meaning some people may need to enroll multiple times over the course of their lives.

Computer Information Attributes

Using computer information characteristics to monitor general data about the PC systems. The data source for these characteristics is WMI (Windows Management Instrumentation).some computer characteristics are shown in Figure (4). [12] and [13].

The Materials and Flow Work Methods

The materials and stream works take two commonly interrelated sides biometric qualities and PC characteristics. Every side has its materials and work process systems.

In biometric attributes, the materials are studies and perform the most types of biometric calculations to choose best one and some modifications are achieved to improve its performance. Computer attributes and numerous of this biometric is accumulated to accomplish coordinating of correlation, encryption and decoding calculations which were examined. Some image handling algorithms is utilized to accomplish to increase the robust of suggested hybrid algorithm and make it more secure. [4]and [5]

To accomplish the authentication and confirmation of the systems and its applications, in biometry, there are two types of biometric strategies. The first is called behavioral biometrics. It is utilized for verification purposes. Verification is figuring out whether a user is who they say they are. This strategy takes a gander at patterns of how certain activities are executed by a person. [6] and [7]

The second called physical biometrics is the other type utilized for identifying or confirmation purposes. Distinguishing proof alludes to figuring out who a user is. This technique is normally utilized as a part of criminal examinations. [12]and [13]

Some algorithms are analysis and discovered the best one and more used in the most e-sports is fingerprints. The edge structures of low quality fingerprints pictures are not generally has very much characterized and, consequently, they cannot be effectively distinguished.

In the suggest algorithm a quick fingerprint developed algorithm is produced, which can enhance the clarity of the edge and valley forms into intended fingerprint pictures in side view of the assessed adjacent ridge direction and occurrences. Fineness index of the separated details and the exactness of an immediately fingerprint conformed framework is used to evaluate the execution of the developed algorithm. The experimental outcomes demonstrate the mixing between human biometric and computer attributes that is produced through hybrid algorithm and using fineness index enhanced the authentication process.[8] and [9]

Fingerprint Enhanced Algorithm

A fingerprint picture improvement algorithm gets a data from input fingerprint pictures through fingerprint scanner device, where number of middle steps is applied to the intended picture, then finally produce the improved picture. so as to present our fingerprint picture improvement algorithm, some of the necessary concepts are given beneath.

The fingerprint picture (I) that has gray level can be characterized as two dimensional array N × N, where, (i, j) represent the pixel intensity of (i-th Row × j-th Column). We expect that every one of the pictures are examined at a resolution of 700 dots for each inch (dpi). The mean and variance of a gray level fingerprint pictures (I) are described in equations (1) and (2) as comparisons.

$$M(I) = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} I(i, j) \quad \text{.....(1)}$$

$$VAR(I) = \frac{1}{N^{2.}} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} (I(i, j) - M(I))^2 \quad \text{.....(2)}$$

The guidance to pictures, P, is characterized as (H ×W) picture, where P(i, j) denotes to a neighborhood edge guidance at pixel (i, j). Thereabout edge guiding (directing) is normally determined for a square as opposed to at each pixel; a picture is isolated into an arrangement of k × k none covering pieces and a solitary neighborhood edge orientation is characterized for every square. In practical experimental which clarifies that the fingerprint picture, where is inequality among a nearby edge guidance of 90^0 and 270^0, because the edges arranged at 90^0 and the edges situated at 270^0 in a nearby neighborhood are not able to separate from one another [15].

A recurrence picture, P, is a (H × W) picture, where P(i, j) denotes to the nearby edge recurrence, that is characterized such as the recurrence of the edge and valley structures of the nearby neighborhood straight is heading ordinary to the neighborhood edge guidance.

The edge and valley structures the nearby neighborhood, that are particulars and solitary focuses [15] show up don't form an all-around characterized sinusoidal-formed wave. Moreover, the circumstances recurrence is characterized as the normal recurrence of the area of the piece (i, j). Similarly, the recurrence pictures indicated piece savvy.

The visor (Mask) V is characterized such as (H × W) a picture, where V(i, j) showing a class of the pixel. A pixel could be either:

1. Non- peak -and-valley (unrecoverable) pixel (with value zero) or
2. Peak -and-valley (recoverable) a pixel (with value one). A specified block wise operation is performed as region masks.

Some primary steps (Figure (3)) performed on fingerprint algorithm to improve and develop its work. The primary steps of the calculation include :

1. **Normalization**: intended fingerprint picture is standardized with the goal that it has an evaluated mean and difference values. Let P(i, j) stands for the dimension level quality at pixel (i, j), M and VAR signify the assessed mean and difference of P individually, and G(i, j) stands for the standardized dark level worth at pixel (i, j).

2. **Orientation Image**

The *orientation picture denotes the characterizations of the fingerprint pictures* and characterizes invariant directions to the edges and valleys in a nearby neighborhood. With the survey a fingerprint picture is a situated surface, various routines have been applied to gauge the guidance scope of unique mark pictures .

3. **Estimation of local trend**: The trend picture is computed from the standardized fingerprint picture.

4. **Estimation of local occurrence**: The frequency picture is discovered from the standardized fingerprint picture and the assessed orientation picture.

5. **Estimation of area mask**: The area cover is obtained by arranging every square in the standardized fingerprint picture into a recoverable or an unrecoverable piece.

6. **Filtering**: A bank of Gabor filters which is tuned to neighborhood edge direction and edge occurrence is connected to the edge and-valley pixels in the standardized fingerprint picture to acquire an improved fingerprint.

Experimental Results of Suggested Algorithm

The purpose of a fingerprint improvement algorithm is to enhance the clarity of ridges and valleys of input fingerprint images and make them more suitable for the minutiae extraction algorithm. The ultimate criterion for evaluating such an enhancement algorithm is the aggregate sum of "value" change when the calculation is connected to the loud fingerprint pictures. Such a change can be estimated subjectively by a visual review of various average improvement results.

Then again, an exact and steady portrayal of the quality change is past the most important object for evaluation. This work has experimental approach based off the enhancement results are shown in Figure (3). For example, the enhanced algorithm has enhanced to be the visibility of the edge and valley structures of fingerprint pictures.

Suggested and Implemented Algorithms

To carry out the work, four interconnected algorithms have been designed and implemented, the results of one algorithm become the entrance to algorithm, which comes after. These algorithms are:

Designed and implemented algorithm to get a fingerprint information and stored in temporary file(**Algorithm (3.1**), Design and implementation of an algorithm to obtain the current characteristics of the computer (**Algorithm (3.2)**, Design hybrid algorithm for encryption the human characteristics and the characteristics of computer attributes **(Algorithm (3.4))** and Decryption algorithm (**Algorithm (3.4)** is designed and implemented: The implemented algorithms are explained as follow.

Algorithm (3.1) (Main Algorithm)

Input

Step one: using user interface to read username, password

Output

Step three make matching to accept or reject the current user

a. if the user accept, he/she can use the network resources (HW/SW)
b. else ,go to step one

Process: **Step two**: test if user stored in DataBase, then perform the following operations

else go to **step Four**

1. Open data base
2. Get required information from DataBase
3. Get computer attributes
4. Go to **Algorithm (3.4) Decryption Algorithm** to execute decryption process and stored information in SQL Database

Step Four: test if the user is new one then go to **Algorithm (3.3) step one**

Algorithm (3.2) (Read attribute & Encrypted Algorithm)

Input

Step one: Open VB6 designed program to get **ReadAttribute** (See figure (4))
Step two: Read current computer attributes (Properties) as in the figure (4)
Output: Mixed Encrypted operation (Ci) between Human Biometric(Mi) and computer attributed (Ki) stored in SQL DataBase.

Process

Step three: Construct concatenate string from computer attributes
Step four: construct message-digest using hash function based MD5 Algo.
Step five: Generate Secret key (Ki) of length (512 byte * 8 bits) from message-digest using MD5 Algorithm
Step six: using RSA Algorithm to Perform Encryption operation using

$$C_i = K_i \oplus M_i \quad \text{Where } \oplus \text{ Encryption operation}$$

Step seven: Store Ci in the SQL DataBase **(DB)**

Algorithm (3.3) (Read Biometric information)

Input:

Step one: turn on the finger printer scanner device
Step two: Read the new person's fingerprint (get fingerprint image)
Output: Encrypted information and stored in SQL DB

Process:

Step one: store fingerprint image in temporary computer memory
Step two: Enhanced fingerprint image using mean filter
Step three: Convert fingerprint image to PMB format
Step four: Convert BMP image Data to blocks of 512 bytes size
Step five: convert 512 bytes in step four to bits streams (512 bytes * 8 bits) as massage (M_i)
Step six: go to Algorithm (3.2) /Step six (to generate keys and make Encryption Process)

Algorithm (3.4) (Decryption Algorithm)

Input

Step one: open SQL DataBase
Step two: Read Required information from DataBase (Ci)
Output: Verification and authentication process of the end user.

Process

Step three: Using VB **ReadAttribute** program to read current computer attributes
Step four: Generate Message digest from computer attributes
Step five: generate secure Key (Ki) based computer attribute and using Hush function
Step six: Perform decryption operation to produce verification information as follow:

$$M_i = C_i \oplus K_i \quad \text{Where } \oplus \text{ is decryption operation}$$

Step seven: matching operation between database information and entered user 's information fingerprinted (thumbprint)

In order to obtain computer attributes, modules programs are built using visual basic language and the results of these programs have ridiculed to gather the computer attributes and then combing them with biometric measurements to produce more complex authentication and authorization for computer networks. Figure (4) Shows some computer attributes which is used in this work.

Results and Discussion

In order to construct the hybrid algorithm to provide protection for networks this suggested and implemented algorithm based on implementing encryption and decryption processes and secret keys generation. The information that has been obtained from the unique humans vital characteristics through finger print algorithm are described in algorithm (3.3), the encryption keys obtained from the unique characteristics(*system type, processor, Bios versions, OS version, Bios Mode,..etc)* of the computer is by using a message-digest algorithm (MDAS) as implemented in algorithm (3.4).A message-digest algorithm is also called a cryptographic hash function. It accepts a message as input (Computer attributes) generates and a fixed-length output, which is generally less than the length of the input message. The output is a hash value, which is used as a secret key (Ki) as implemented in the algorithm (3.2) step three. Message-digest algorithm is used to make the suggested algorithm satisfies the following properties:

a. It should be one-way. Given the message digest, it is hard to get the original message.

b. Given both input and output, it is difficult to find another input message that generates same output.

c. It should be collision-resistant. It is computationally infeasible to find two messages (Two computers attributes), which generates the same message digest. The message digest should satisfy pseudo-randomness. Experimental results show that all of the above properties are satisfied, The MD5 algorithm is used to generate secret Keys (Ki) based on computer attributes as shows in figure (4). MD5 is used because it has the following properties, Bitwise Boolean Operation, Modular Addition and Cyclic Shift Operation; Experimental results show that these three operations are very fast on a 64-bit machine. Therefore, MD5 is quite fast and more accurate.

MD5 (message digest algorithm) hashes are one-way functions that produce a "fingerprint". Essentially, they map something with many bits down to just a few bits (128 in the case of MD5) in such a way that collisions are as rare as possible. In cryptography, one-way hashes are used to verify something without necessarily giving away the original information; Experimental results show the complexity of proposed technique which is achieved.

To implement the hybrid Algorithm , Human Biometric information is used to generate messages (Mi) of length (512) byte, EAS Algorithm is used to encrypt the message (Mi) using secret key (Ki) That has been generated from computer properties as a digest message as implemented in Algorithm(3.3).

The authentication and verification process is implemented and executed according to algorithm (3.1) . and it is archived in two separate sides ,the first side is matching user information with SQL database to allow user access by executing decryption process (shown in Algorithm (3.4**)**) and read the current computer properties ,the second side is reading new fingerprint image through finger print scanner device and computer properties and execute all the algorithms described above.

The accuracy and reliability of a biometric fingerprint recognition that is based on the experimental can be described as follow:

with a view to ensure that the performance of fingerprint identification/verification technique will be robust with respect to the quality of input fingerprint images by using mean filter, it is fundamental to combine a fingerprint enhancement algorithm in the minutiae extraction module. We present a fast fingerprint enhancement algorithm, which can adaptively improve the clearance of ridge and hollows structures of input

fingerprint images based on the estimated local ridge direction and hesitation. The local and global structures of minutiae together provide a solid basis for reliable and robust minutiae matching. Experimental results show the proposed minutiae matching scheme is suitable for an online processing due to its high processing speed. We have assessed the performance of the image enhancement algorithm using the goodness index of the extracted minutiae and the accuracy of an online fingerprint verification module. Experimental results show that incorporating the enhancement algorithm improves both the goodness index and the verification accuracy.

Summary and Conclusions

A current electronic security system, which is depending on individual recognizable proof to guarantee that a user is an approved client of a system, has a typical powerlessness: the verification can be copied. which can be almost dispensed with utilizing biometrics. Different associations to expand security levels and ensure their information and licenses can utilize biometrics.

References

1. Maio, D.; Maltoni, D.; Cappelli, R.; Wayman, J. L. and Jain. A. K. FVC(2004) Third Fingerprint Verification Competition. In Proceedings of International Conference on Biometric Authentication, pages 1–7, Hong Kong, China, July 2004.

2. Foster, C.; Kesselman, S. and Tuecke, "The anatomy of the grid: enabling scalable virtual organizations", Int. J. High Performance Computing, NIST Internal Report 7123; available at http://fpvte.nist.gov/report/ir_7123_summary.pdf, June 2004.

3. Quan Zhou; Geng Yang; Jian Shegang n and Chunming Rong, ,(2005), "A Scalable Architecture for Grid", Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies

4. Huynh Crystal; Brunelle Erica; Halámková Lenka; Agudelo Juliana and Halámek Jan (2015). "Forensic Identification of Gender from Fingerprints". Analytical Chemistry(journal) **87** (22):1153111536. doi:10.1021/acs.analchem.5b03323.Retrieved 21 November 2015.

5. Hwang, T.; Chen, Y. and Laih, C.S.,(2007), "Non-Interactive password authentication without password tables", IEEE Conference on Computer and Communication Systems,. 429-431.

6. Lee, J.K.; Ryu, S.R. and Yoo, K.Y.(2002). "Fingerprint-based remote user authentication scheme using smart cards", Electron. Lett , 38,12, 554-555.

7. Chang, C.C. and Lin, I.C. (2004), "Remarks on fingerprint-based remote user authentication scheme using smart cards", ACM SIGOPS operating System Rev., 38, 4, 91-96.

8. Lin, C.H. and Lai,Y.Y. (2004) ,"A flexible biometrics remote user authentication scheme", Computer Standards Interfaces, 27, 1, 19-23.

9. Davide Maltoni; Durio Maio; Anil, K. Jain and Salil Prabhakar, (2002) ,Handbook of Fingerprint Recognition, Prentice Hall.

10. Ruud M. Bolle; Jonathan H. Connell; Sharath Pankantiand Nalini K. Ratha, 2003, Andrew W. Senior, Guide To Biometrics, John Wiley & Sons,

11. Dodis Y.; Ostrovsky, R.; Reyzin, L. and Smith, A. (2008) "Fuzzy extractors: How to generate strong keys from biometrics and other noisy", Appears in SIAM Journal on Computing, 38(1):97–139,

12.Uludag U; Pankanti S.,Prabhakar, and Jain, A. K., (2004). "Biometric cryptosystems: Issues and challenges," Proc. IEEE, Special Issue on Multimedia Security for Digital Rights Management, 92, 6, 948–960.

13. Angle, S. ; Bhagtan, R. and Chheda, H. (2005) ," BIOMETRICS : A FURTHER ECHELON OF SECURITY", UAE International Conference on Biological and Medical \\ldots

14. Åström Paul,(2007)"The study of ancient fingerprints" (PDF). Journal of Ancient Fingerprints (1) .

15. Wang Yongchang; Hao, Q.; Fatehpuria, A.; Lau, D. L and Hassebrook, L. G. (2009). "Data Acquisition and Quality Analysis of 3Dimensional Fingerprints" (PDF). Florida: IEEE conference on Biometrics, Identity and Security. Retrieved March(2010).

Table (1): Classifications of Biometrics [13]

Biometrics Type Recognition	Matching Biometric	description
DNA	Chemical	The ID of an individual utilizing the investigation into fragments of DNA
Ear	Visual	The ID of an individual utilizing the state of the ear
Eyes(Iris)	Visual	Utilization of the elements found in the iris to distinguish a person
Retina	Visual	Utilization of veins in the back of the eye to perform acknowledgment
Face	Visual	The examination of facial components of a singular's personality
Fingerprint	Visual	The utilization of the edges and valleys found at first glance tips of a human finger to recognize a person.
Finger Geometry	locative	Utilization of 3D geometry of the finger to focus character
Track	Reconnoiter	Utilization of a singular's strolling style or walk to determine identity
Hand Geometry	Spatial	Utilization of the geometric components of the hand
Odour	Behavioral	Utilization of a singular's scent to determine identity
Signature	Behavioral	The validation of a person by the investigation into penmanship style

Table :(2) Comparing biometric types. [7]

BIOMETRIC TYPE	Fingerprint	Facial Recognition	Hand Geometry	Speaker Recognition	Iris Scan	Retinal Scan
Verification	✓	✓	✓	✓	✓	✓
Identification	✓	×	×	×	✓	✓
Accuracy (4)	4	3	3	2	4	4
Reliability(4)	3	2	2	1	3	3
Security Level (4)	3	2	2	2	3	3
Longterm Stability (4)	3	2	2	2	3	3
Acceptance (4)	2	2	2	3	2	2
Ease of Use (4)	3	2	3	3	2	1

Table (3) Biometric Devices [4]

Device	Description Use
Retina Scanner	These scan the interesting biometric example in every individual's iris, and match it against a specific number of novel distinguishing denote that set each individual separated from other people.
Iris checking	Retinal examining are used to distinguish a man as indicated by their remarkable pattern; however they have a tendency to be far costlier and more complicated.
FingerPrint Scanner	-As far as value goes, the unique mark examining is on the lower end of the scale. The least expensive fingerprint scanners are the ones that just scan the genuine print; however, the costlier ones really examine the vicinity of blood in the finger impression, the size and state of the thumb, and numerous different components.
Facial Biometrics	Each individual around the world has a particularly one of a kind face, even two twins that the human eye cannot differentiate one from the other. It might be something as little as the somewhat diverse putting of the eyebrows, the width of the eyes, or the breadth of the nose.
Voice Recognition	Every person has a one of a kind voice pattern, despite the fact that the progressions are slight and scarcely perceptible to the human ear. Those little contrasts in every individual's voice can be noted, tested, and authenticated to just permit access to the individual that has the right tone, pitch, and volume of voice.
Hand Print Patterns	When you put your hand on a scanner, you have a special unique fingerprint design, as well as the size and state of your whole hand is likewise extremely unique

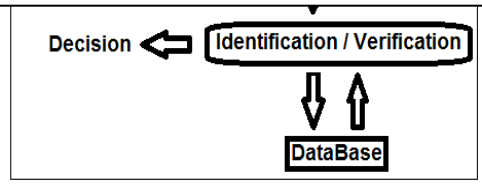

Figure (1). Basic biometric authentication system.

Figure (2) General Fingerprint Patterns

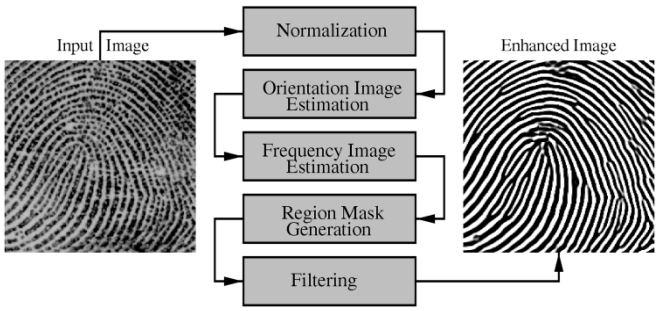

Figure (3) Fingerprint Enhancement Algorithm

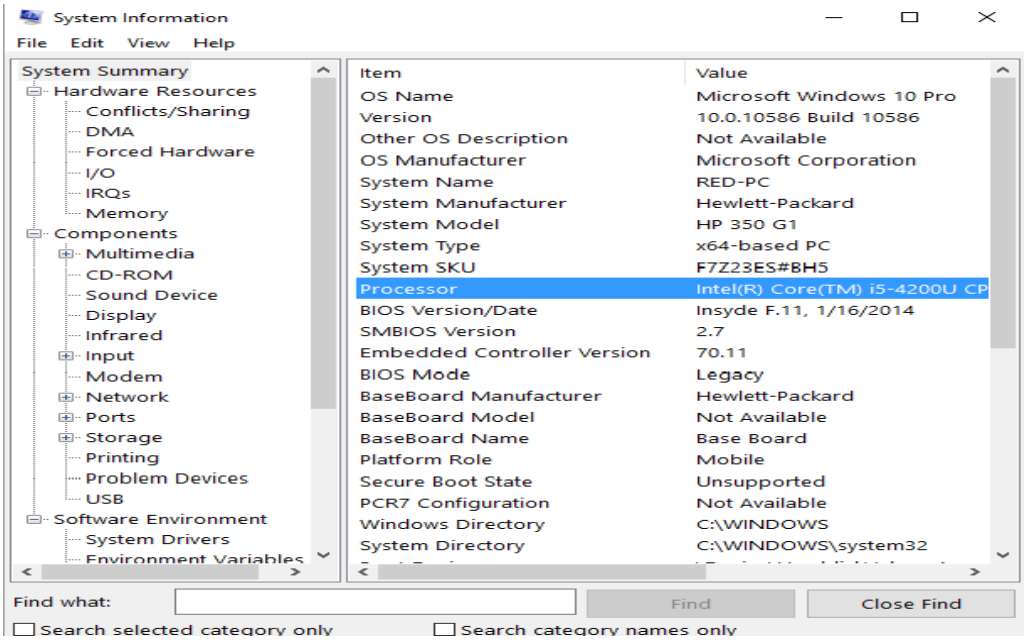

Figure (4) Computer Attributes: H/W resources, S/W Environment and Components

خوارزمية هجينة لحماية شبكات الكومبيوتر اعتمادا" على القياسات الانسان وسمات الكومبيوتر

رحيم عبد الصاحب عكلة

قسم علوم الحاسبات/ الجامعة التكنولوجية

استلم في :26/كانون الثاني/2016قبل في :3/تشرين الاول/2016

الخلاصة

الغرض من هذا العمل هو الخلط بين الخصائص البيومترية البشرية وخصائص الحاسوب الفريدة من اجل حماية بيئات شبكات الحاسوب ومواردها من خلال تطويرتقنيات أثبات الأصل والتفويض.في الجانب البيومترية البشري، تم دراسة أفضل الطرائق والخوارزميات المستعملة، وكان الأستنتاج هو إن البصمة تعد ألافضل ، ولكنها تحتوي على بعض العيوب. خوارزمية بصمة تم تحسين أدائها اذ يمكن تكيفها لتعزيز وضوح حافة واخدود هياكل صور البصمة مع الأخذ بالحسابات لتقييم إدخال الحافة القريبة وتكرار.
في الجانب مميزات الكمبيوتر، الكمبيوتر ومكوناته مثل الإنسان له خصائص فريدة مشابه للخصائص البايلوجية، في هذا الجانب، تم أعداد برنامج في البيئة الفجول بسك، هدف هذا البرنامج للحصول على خصائص جهاز الكمبيوتر ودمجها مع الخصائص البشرية للحصول على خوارزمية هجينة لتحقيق المصادقة والتخويل يمكن الاستفادة منها لحماية بيئات شبكات الحاسوب والمصادر المخزونة في الخوادم من خلال إنشاء وحدات برمجية وواجهات تفاعلية لتحقيق هذا الغرض.

الكلمات المفتاحية: القياسات الحيوية، ميزات القياسات الحيوية، المصادقة والاعتمادية، امنية الحاسوب، خصائص الحاسوب، التشفير / فك التشفير ، بصمات الأصابع