STM JOURNALS

Journal of Image Processing & Pattern Recognition Progress

Volume 1, Issue 2
www.stmjournals.com

Multi-Modal (Hybrid) More Efficient and Highly Secured Enhanced Hand Geometry Authentication using 3 Steps Authentication by Means of Biometrics, Steganography and Encryption

*Nader A. Rahman Mohamed**
Department of Biomedical Engineering, Faculty of Engineering, Misr University for Science and Technology (MUST), Egypt

Abstract

"Biometrics" is the science, which is used to verify the identity of the persons through either behavioral traits or physical characteristics. This area has gained great importance in maintaining the security of the places that require high security accuracy. Hand geometry is considered one of the biometrics, which derived its reputation from the ease of use and the acceptance of many people to use it. Hand geometry based biometric systems are gaining acceptance in low to medium security applications. Hand biometrics is extensively used for personal authentication. The widespread dissemination of verification systems using biometrics and continuous attempts to break the security of these systems, such as the use of fingerprints rubber to break the security systems that use fingerprint, or use a voice recorder to break the security systems that use voice tag, and so on. Although the efficiency of biometrics in identification of people is very accurate and highly secured, but still the data concerning it is not a secret, and if it is compromised, it would compromise the integrity of the system where protection is required. Protecting biometric data has become an important issue, so that it cannot be misused by attackers. In order to increase security of biometric data there are different methods in which digital steganography could be widely accepted. Steganography is defined as the science of hiding or embedding information in a transmission medium in a way to be undetectable by observers. To address these issues, this paper proposes a novel encryption method with password protection based on an enhanced version of multi-modal hand geometry authentication using three authentication layers based on hand geometry verification, digital steganography, and password encryption.

Keywords: *Biometrics, hand geometry authentication, digital steganography*

**Author for Correspondence* E-mail: nader_mohamed@hotmail.com

INTRODUCTION

Any biometric system mainly consists of three main modules. The first one is the data acquisition module, which is a sensor that captures the biometric data and converts it to a digital form like image, audio, video, etc. The second module is the feature extraction module, in which some significant features are extracted from acquired biometric, forming what is called "Feature Vector." This feature vector is stored in the biometric system during enrollment phase, and represents the user's identity and is well known as "template." The third main module is the matching module, which compares the extracted feature vector with the second module during authentication phase with respect to the stored feature vector "template" during enrollment phase, and accordingly authenticates or denies access.

Figure 1 shows the three main modules which consist of any biometric system, and the eight major attempts to break the security of the biometric system.

1. A fake biometric trait such as an artificial organ may be presented at the sensor.
2. Illegally intercepted data may be resubmitted to the system.

3. The feature extractor may be replaced by a Trojan horse program that produces pre-determined feature sets.
4. Legitimate feature sets may be replaced with synthetic feature sets.
5. The matcher may be replaced by a Trojan horse program that always outputs high scores thereby defying system security.
6. The templates stored in the database may be modified or removed, or new templates may be introduced in the database.
7. The data in the communication channel between various modules of the system may be altered.
8. The final decision may be overridden.

Therefore, protecting biometrics against fraud attacks has become an important issue nowadays. One of the solutions to this problem has been introduced here in this paper, by tagging the biometric with one of the oldest, well-known, and conventional method of security, which is PIN code, but in a way to be hidden and secured by the sake of the robustness of steganography. Figure 2 illustrates the interrelation between biometrics and the embedded image security in a way to enhance user convenience and boost security. The system in such a design can be highly protected against various types of previously mentioned threats.

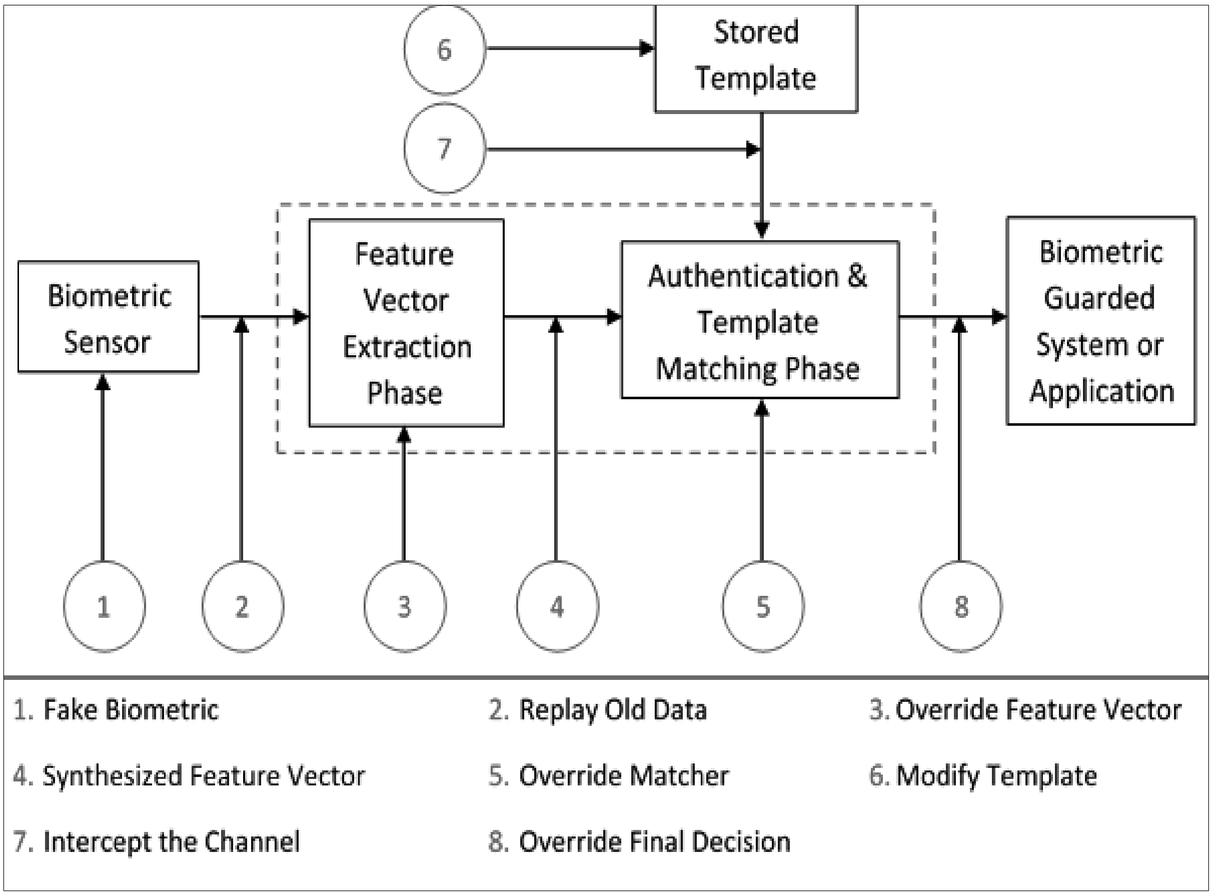

6
Stored Template
7
Biometric Sensor
Feature Vector Extraction Phase
Authentication & Template Matching Phase
Biometric Guarded System or Application
1
2
3
4
5
8
1. Fake Biometric
2. Replay Old Data
3. Override Feature Vector
4. Synthesized Feature Vector
5. Override Matcher
6. Modify Template
7. Intercept the Channel
8. Override Final Decision

Fig. 1: *Various Risk Attacks while Using any Biometric System.*

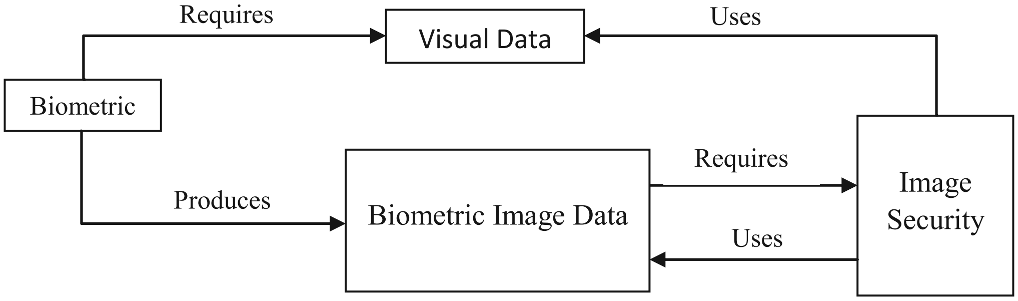


Fig. 2: *Relation between Biometrics and Image Security.*

Biometrics

The need to identify people is as old as humankind. People recognize each other by sight and sound. However, in today's complex society, it is impossible to personally know everyone.

Automatic human identification has become an important issue in today's information and network-based society. The techniques for automatically identifying an individual based on his physiological characteristics are called biometrics, which provide an answer to this need.

Biometric devices automate the personal recognition process. Each of us is unique from every other human being. We have unique physical characteristics, such as hand shape, blood vessel patterns and fingerprints. Biometric devices measure and record these characteristics for automated comparison and verification. Biometric identification is, simply, the technique of verifying a person by a physical characteristic or personal trait. Our brains perform biometrics in distinguishing our associates from our family although, occasionally, there may be similarities.

Biometric techniques fall into two categories: physiological and behavioral. Common physiological biometrics include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and geometry, wrist veins or thermal images. Behavioral biometrics includes voiceprints, handwritten signatures and keystroke/signature dynamics. Behavioral biometric technologies are less expensive to implement than physical biometric systems, but they are also less robust. They are more susceptible to rejection due to carelessness, high emotional states, illness, drugs, and so forth.

Several factors determine which method best suits an organization. The methods offer varying degrees of effectiveness, and typically, implementation cost varies with the level of security provided. Specialized hardware, for example, drives up the price rapidly, while solutions that can use common hardware cost thousands less.

Beyond cost and effectiveness, companies must consider the psychological implication these techniques have for employees. With this in mind, the ideal biometric would be easy to use, noninvasive, convenient and socially acceptable.

Hand geometry is considered one of the biometrics, which derived its reputation from the ease of use and the acceptance of many people to use it. Hand geometry-based biometric systems are gaining acceptance in low to medium security applications. Hand biometrics is extensively used for personal authentication [1, 2].

Steganography

Steganography is the art of hiding or embedding information in a transmission medium in a way to be undetectable by observers.

In the present case, the transmission media will be the hand image, and the embedded information will be the PIN code.

The idea is hiding the PIN code with steganography methods reduces the chance of a PIN code being detected. However, if that code is also encrypted, if discovered, it must also be cracked (yet another layer of protection) [3, 4].

The steganographic process can be described with the following formula:

Cover medium + Data to hide = Stego Medium

In a 24-bit image, there is 3 byte of data to represent RGB values for every pixel in that image. This implies that we can store/hide 3 bit in every pixel. For example, if the image has the following bits:
10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

To store ***101101101,*** we replace with the original LSBs like this:
1001010**1** 0000110**0** 1100100**1**
1001011**1** 0000111**0** 1100101**1**
1001111**1** 0001000**0** 1100101**1**

The underlined bits are the only four actually changed in the 9 bytes used. To reveal the stored message, the LSBs are extracted alone from the stego medium and combined together.

SYSTEM DESCRIPTION

As any working biometric system, the automatic hand geometry verification system (AHVS) consists of both hardware and software; the hardware captures the human hand image, and the software drives the hardware, extracts measurements of the hand based on the proposed 45-point model of the hand, interprets the resulting data and determines acceptability [5].

There are two distinct phases of operation for any biometric system: enrollment and verification/identification. In the first phase, identity information from users is added to the system. In the second phase, live biometric information from users is compared with stored records. The crucial step in building any effective biometric system is enrollment. If the enrollment templates are of poor quality, it will affect the subsequent performance of the system. During enrollment, each user provides samples of that system's specific biometric characteristic by interacting with the scanning hardware.

The capturing device used to capture the image of the hand, in either the enrollment phase or the verification phase, is an infrared CCD camera located in a compartment where the user can put his hand. The compartment is about 24.5 cm wide, 24.5 cm deep and 20 cm high, and the distance between camera lens and the normal projection point, along the optical axis, on the lower horizontal board is about 17 cm. The camera is attached to a cooling fan, because the ICs get very hot after using the camera for a short time. As an example, the user puts his hand in front of the camera to be captured, after he enters his PIN code. The system then extracts the appropriate features like finger lengths, finger areas, and finger widths at different heights of the different fingers of the right hand as well as the radius of the hand center from the scan. After three successive enrollments, the system stores the mean data as a template, then the user is prompted to enter his pass key, which will be used later to tag the biometric hand image as a hidden pass key.

The next time the user tries to access using the system during the verification phase, his hand is scanned again by the camera, after he enters his PIN code correctly, then the hardware passes the data to the software, which checks the user templates. If there is a match, the user will be asked for his pass key, which will also be checked against the hidden pass key which will be extracted from the previously tagged biometric hand image, if still there is a match, he is granted access; otherwise, the system asks him to align his hand and re-scan it "in case of mismatch with stored template" or to re-enter the pass key "in case of mismatch with the hidden pass key." If there is no match up to three times, a message reports that the system cannot verify the user.

Four major steps can describe the automatic hand geometry verification system (AHVS)

Data Acquisition Stage

This is the first stage in the automatic hand geometry verification system (AHVS), where acquiring the hand image takes place. It is done using an infrared camera attached to a video card, connected to the computer.

The user locates the right hand, guided by five marks in the camera compartment; where the hand is to be placed, to ensure that users place their hands in a controlled way so as to guarantee higher verification rate. These marks replace the pegs in other older systems, as a result no impression can be found on the hand skin, and measured dimensions are accurate. Figure 3 shows the five marks with respect to the hand.

The camera captures the image of the human hand and sends the captured image to the computer software, which in turn interprets the resulting data and determines acceptability.

Preprocessing Stage

This is the second stage in the automatic hand geometry verification system (AHVS). It mainly consists of four consecutive sub-stages, namely, segmentation (i.e., binarization), boundary detection, thinning and tracing. Figure 4 illustrates the block diagram of the preprocessing stage.

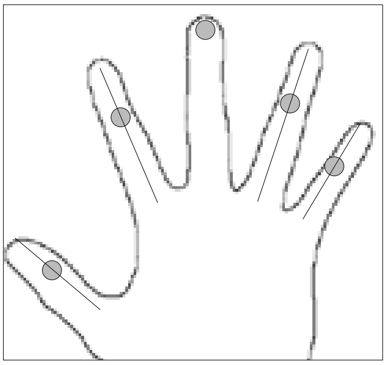


Fig. 3: *Location of the Hand over the Marks in the AHVS.*

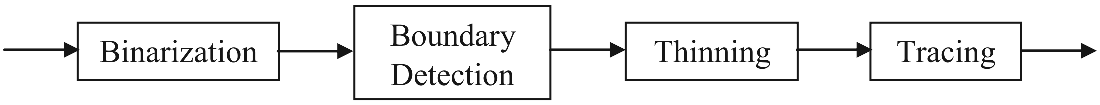


Fig. 4: *Block Diagram of Preprocessing Stage.*

Binarization

Binarization is the process of segmenting the image into two levels: object and background; the object segment which is the hand in black and the background segment in white.

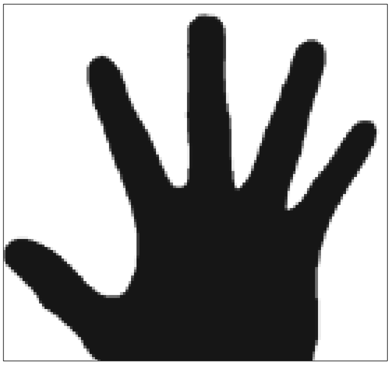


Fig. 5: *Result of Binarization Sub-Stage.*

The algorithm used in the binarization sub-stage is an iterative method used for calculating and selecting an optimal threshold, which is used to segment the image into two distinct parts: hand and background.

Boundary Extraction

Boundary detection or boundary extraction is the next sub-stage after binarization takes place. It is done by examining the black pixels and their 8-neighborhood.

If the pixel is black, and all its 8-neighborhood are white, then the central pixel is a noisy pixel, and is changed to white. If the pixel is black and all its 8-neighborhood are black then the central pixel is an interior pixel in the hand and is changed to white, otherwise it is a boundary pixel and remains black.

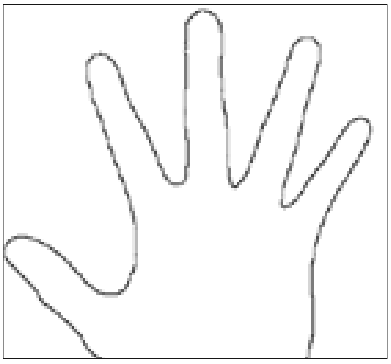


Fig. 6: *Result of Boundary Detection Sub-Stage.*

Boundary Thinning

Thinning of the boundary is performed to guarantee that the boundary of the hand is one pixel wide. This step is necessary and prerequisite for the next step "boundary tracing."

The thinning approach removes boundary pixels of a connected component that are neither essential for preserving the connectivity nor do they represent any significant geometrical features.

The thinning algorithm is designed based on parallel thinning and satisfies the following criteria:

Criterion 1: A fully parallel operator should require only one pass per iteration.

Criterion 2: Connectivity should be preserved for both sets of pixels whose value is 1 and 0 defined over a rectangular tessellation, respectively. Connectivity is defined as follows: two 1's are connected if they are 8-connected, and two 0's are connected if they are 4-connected.
Criterion 3: Skeleton should be invariant under translation and rotation of integer multiple of 90 degrees.
Criterion 4: Skeleton should converge to unit width.
Criterion 5: Skeleton should closely approximate to their medial axes.
Criterion 6: Skeleton should be insensitive to boundary noise.

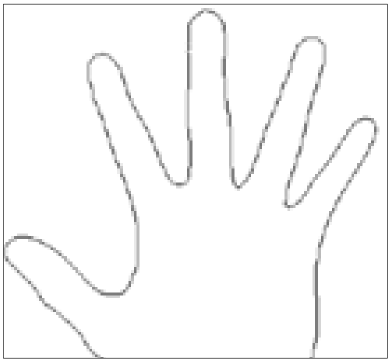
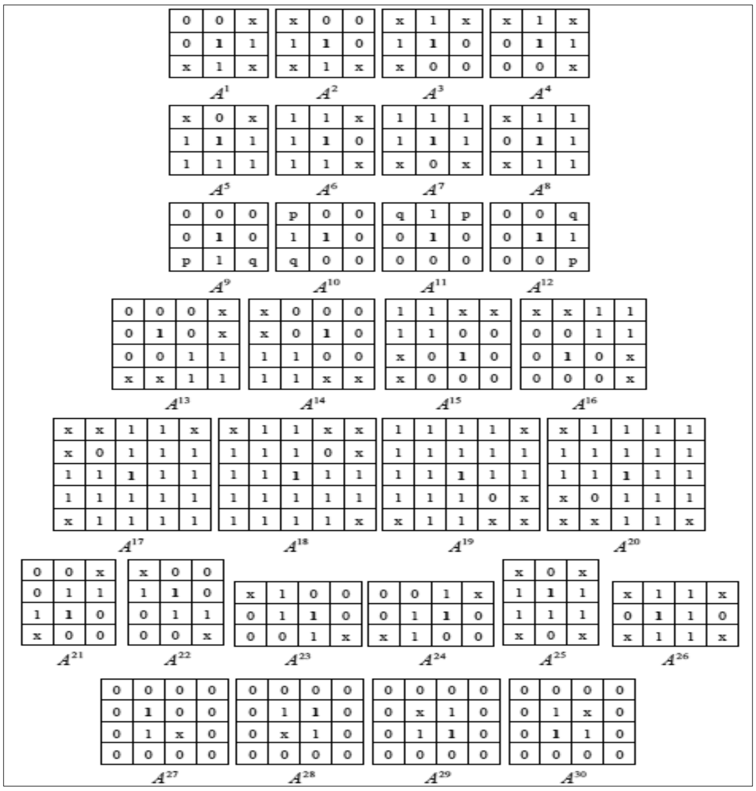


Fig. 7: *Result of Boundary Thinning Sub-Stage.*

The algorithm uses 30 templates, which are shown in Figure 8. Templates 1–20 are called thinning (deleting) templates while templates 21–30 are called restoring templates [6].

Templates 1–4 remove corners from all four directions, whereas templates 5–8 remove 4-connected boundary pixels; they remove pixels evenly from all directions. Templates 9–16 are a set of noise cleaning templates and are used to suppress the growth of noisy skeletons induced by boundary noise of unit size. 5 × 5 templates 17–20 are used to ensure the generation of isotropic skeletons at right angle corners.

Boundary Tracing
For tracing the boundary of the hand to construct an x-y array for the hand boundary in sequence, the sequence starts from one end (E1), then to fingers and finally the other end (E2), where the two ends are proximal to the wrist at the lower bound of the image; refer to Figure 11. After that a conversion of the x-y array to r-θ "polar coordinates" takes place, with respect to the origin point (O), where this origin (O) is taken at the halfway point between the two ends.



0	0	x
0	1	1
x	1	x

A^{1}

x	0	0
1	1	0
x	1	x

A^{2}

x	1	x
1	1	0
x	0	0

A^{3}

x	1	x
0	1	1
0	0	x

A^{4}

x	0	x
1	1	1
1	1	1

A^{5}

1	1	x
1	1	0
1	1	x

A^{6}

1	1	1
1	1	1
x	0	x

A^{7}

x	1	1
0	1	1
x	1	1

A^{8}

0	0	0
0	1	0
p	1	q

A^{9}

p	0	0
1	1	0
q	0	0

A^{10}

q	1	p
0	1	0
0	0	0

A^{11}

0	0	q
0	1	1
0	0	p

A^{12}

0	0	0	x
0	1	0	x
0	0	1	1
x	x	1	1

A^{13}

x	0	0	0
x	0	1	0
1	1	0	0
1	1	x	x

A^{14}

1	1	x	x
1	1	0	0
x	0	1	0
x	0	0	0

A^{15}

x	x	1	1
0	0	1	1
0	1	0	x
0	0	0	x

A^{16}

x	x	1	1	x
x	0	1	1	1
1	1	1	1	1
1	1	1	1	1
x	1	1	1	1

A^{17}

x	1	1	x	x
1	1	1	0	x
1	1	1	1	1
1	1	1	1	1
1	1	1	1	x

A^{18}

1	1	1	1	x
1	1	1	1	1
1	1	1	1	1
1	1	1	0	x
x	1	1	x	x

A^{19}

x	1	1	1	1
1	1	1	1	1
1	1	1	1	1
x	0	1	1	1
x	x	1	1	x

A^{20}

0	0	x
0	1	1
1	1	0
x	0	0

A^{21}

x	0	0
1	1	0
0	1	1
0	0	x

A^{22}

x	1	0	0
0	1	1	0
0	0	1	x

A^{23}

0	0	1	x
0	1	1	0
x	1	0	0

A^{24}

x	0	x
1	1	1
1	1	1
x	0	x

A^{25}

x	1	1	x
0	1	1	0
x	1	1	x

A^{26}

0	0	0	0
0	1	0	0
0	1	x	0
0	0	0	0

A^{27}

0	0	0	0
0	1	1	0
0	x	1	0
0	0	0	0

A^{28}

0	0	0	0
0	x	1	0
0	1	1	0
0	0	0	0

A^{29}

0	0	0	0
0	1	x	0
0	1	1	0
0	0	0	0

A^{30}

Fig. 8: *Thinning Templates.*

Feature Extraction Stage

Feature extraction stage is the third stage in the automatic hand geometry verification system (AHVS). At the end of this stage, a feature vector becomes available to be passed to the matching stage, where it is compared with the appropriate template to generate a decision whether this hand is accepted or not.

Extraction of the hand geometry characteristic features is based on anatomical landmarks “fingertips and bottom of valleys between fingers.” Figure 9 illustrates these anatomical landmarks.

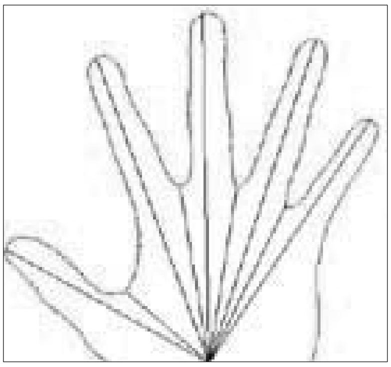


Fig. 9: *Fingertips and Bottom of Valleys between Fingers.*

After the determination of nine points corresponding to the fingertips and bottom of valleys between fingers (steps 1, 2; Table 1) a complete set of 45 points is located.

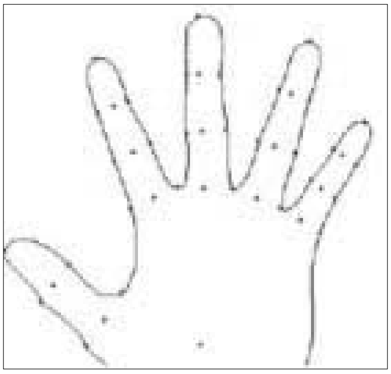


Fig. 10: *The Complete Set of the 45 Anatomical Landmarks.*

Then thirty distances, circumference and area measures are extracted automatically based on these 45 points (refer to Table 2).

These features (distances, circumferences and areas) are the finger lengths, finger circumferences, finger areas, and finger widths at different positions of the different fingers of the right hand as well as the radius of the circle describing the palm of the hand.

The determination of the proposed 45 points of the hand geometry model is illustrated in Figure 11 and Table 1.

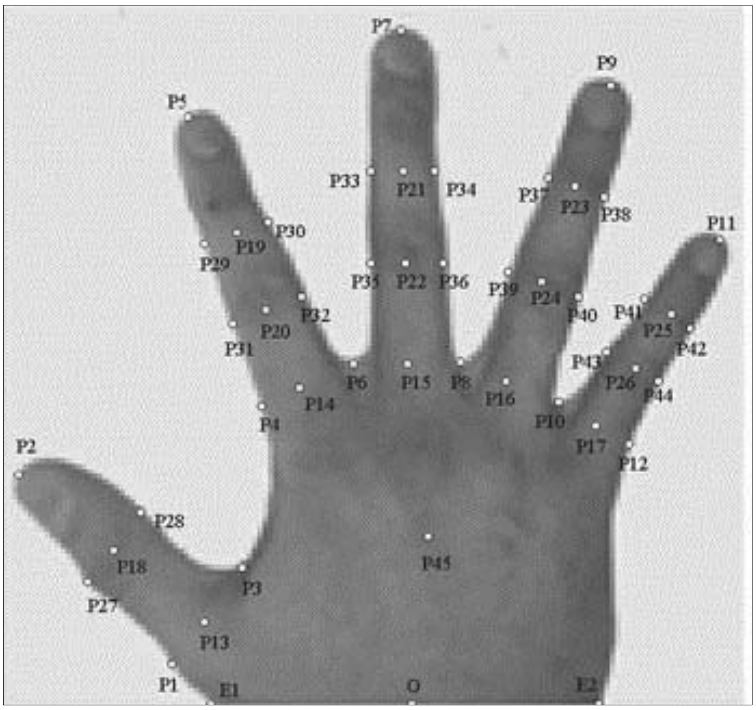


Fig. 11: *The 45 Anatomical Landmarks of Proposed Hand Geometry Model.*

Table 1: *Steps of Determination of the 45 Anatomical Landmarks.*

Step No.	Step Description
Step 1	Locating 5 fingertips: P2, P5, P7, P9 and P11
Step 2	Locating 4 bottoms of valleys between fingers: P3, P6, P8 and P10
Step 3	Locating fingers base remaining points (side points): □ P1 such that the distance between P2 and P1 equals the distance between P2 and P3 □ P4 such that the distance between P5 and P4 equals the distance between P5 and P6. □ P12 such that the distance between P11 and P12 equals the distance between P11 and P10.
Step 4	Locating the 5 fingers bases (center points): □ P13 half the way between P1, P3. □ P14 half the way between P4, P6. □ P15 half the way between P6, P8. □ P16 half the way between P8, P10. □ P17 half the way between P10, P12.
Step 5	Locating the 9 remaining finger axis points: □ P18 half the way between P2, P13. □ P19 one-third the distance between P5, P14. □ P20 two-thirds the distance between P5, P14. □ P21 one-third the distance between P7, P15. □ P22 two-thirds the distance between P7, P15. □ P23 one-third the distance between P9, P16. □ P24 two-thirds the distance between P9, P16. □ P25 one-third the distance between P11, P17. □ P26 two-thirds the distance between P11, P17.
Step 6	Locating the 18 remaining finger boundary points: □ P27 between P2, P1 such that the line P18–P27 is perpendicular to the line P2–P13 □ P28 between P2, P3 such that the line P18–P28 is perpendicular to the line P2–P13 □ P29 between P5, P4 such that the line P19–P29 is perpendicular to the line P5–P14 □ P30 between P5, P6 such that the line P19–P30 is perpendicular to the line P5–P14 □ P31 between P5, P4 such that the line P20–P31 is perpendicular to the line P5–P14 □ P32 between P5, P6 such that the line P20–P32 is perpendicular to the line P5–P14 □ P33 between P7, P6 such that the line P21–P33 is perpendicular to the line P7–P15 □ P34 between P7, P8 such that the line P21–P34 is perpendicular to the line P7–P15 □ P35 between P7, P6 such that the line P22–P35 is perpendicular to the line P7–P15 □ P36 between P7, P8 such that the line P22–P36 is perpendicular to the line P7–P15 □ P37 between P9, P8 such that the line P23–P37 is perpendicular to the line P9–P16 □ P38 between P9, P10 such that the line P23–P38 is perpendicular to the line P9–P16 □ P39 between P9, P8 such that the line P24–P39 is perpendicular to the line P9–P16 □ P40 between P9, P10 such that the line P24–P40 is perpendicular to the line P9–P16 □ P41 between P11, P10 such that the line P25–P41 is perpendicular to the line P11–P17 □ P42 between P11, P12 such that the line P25–P42 is perpendicular to the line P11–P17 □ P43 between P11, P10 such that the line P26–P43 is perpendicular to the line P11–P17 □ P44 between P11, P12 such that the line P26–P44 is perpendicular to the line P11–P17
Step 7	Locating the center of the circle P45 passing by P6, P8 and P10

Out of these 45 points, thirty different features are extracted, and selected to represent the hand geometry. These features which are discussed in Table 2; twenty-five of them are distances of the length, width and circumference of the fingers while the remaining five are derived from the finger areas.

The measurements can be in terms of millimeters, inches, or pixels. The last one is selected and the conversion to millimeters or inches is straightforward.

There are 25 measurements in Table 2 which are 1-D measurements, while the other 5 measurements are related measures of areas. And as the area itself is considered as a 2-D measurement, so, the square root of an area is selected as a measure of an area, since that will make the 30 measurements homogenous in terms of 1-D numbers.

Table 2: *Features used for Hand Verification.*

Feature No.	Feature Description
F1	Distance between P1, P3
F2	Distance between P27, P28
F3	Distance between P2, P13
F4	Distance between P4, P6
F5	Distance between P31, P32
F6	Distance between P29, P30
F7	Distance between P5, P14
F8	Distance between P6, P8
F9	Distance between P35, P36
F10	Distance between P33, P34
F11	Distance between P7, P15
F12	Distance between P8, P10
F13	Distance between P39, P40
F14	Distance between P37, P38
F15	Distance between P9, P16
F16	Distance between P10, P12
F17	Distance between P43, P44
F18	Distance between P41, P42
F19	Distance between P11, P17
F20	Distance between P45, P8
F21	The square root of the area of the thumb finger
F22	The square root of the area of the index finger
F23	The square root of the area of the middle finger
F24	The square root of the area of the ring finger
F25	The square root of the area of the little finger
F26	The circumference of the thumb finger along the path defined by the points: P1, P27, P2, P28, P3 and P1
F27	The circumference of the index finger along the path defined by the points: P4, P31, P29, P5, P30, P32, P6 and P4
F28	The circumference of the middle finger along the path defined by the points: P6, P35, P33, P7, P34, P36, P8 and P6
F29	The circumference of the ring finger along the path defined by the points: P8, P39, P37, P9, P38, P40, P10 and P8
F30	The circumference of the little finger along the path defined by the points: P10, P43, P41, P11, P42, P44, P12 and P10

Tagging Biometric Image

As mentioned earlier, this paper is presenting a solution for protecting biometric system by tagging the biometric image with a hidden key using both steganography and encryption techniques, to raise the level of security three times more than regular biometric authentication.

In the preprocessing stage, precisely after the boundary tracing, x-y array for the hand boundary in sequence is constructed, and this will be our first step to hide the pass key!

This array will be used to locate hand boundary pixels in the original hand image in which we will hide the user's pass key.

Hand Image with Boundary Pixels Detected

+

User's Pass key to Hide

⊕

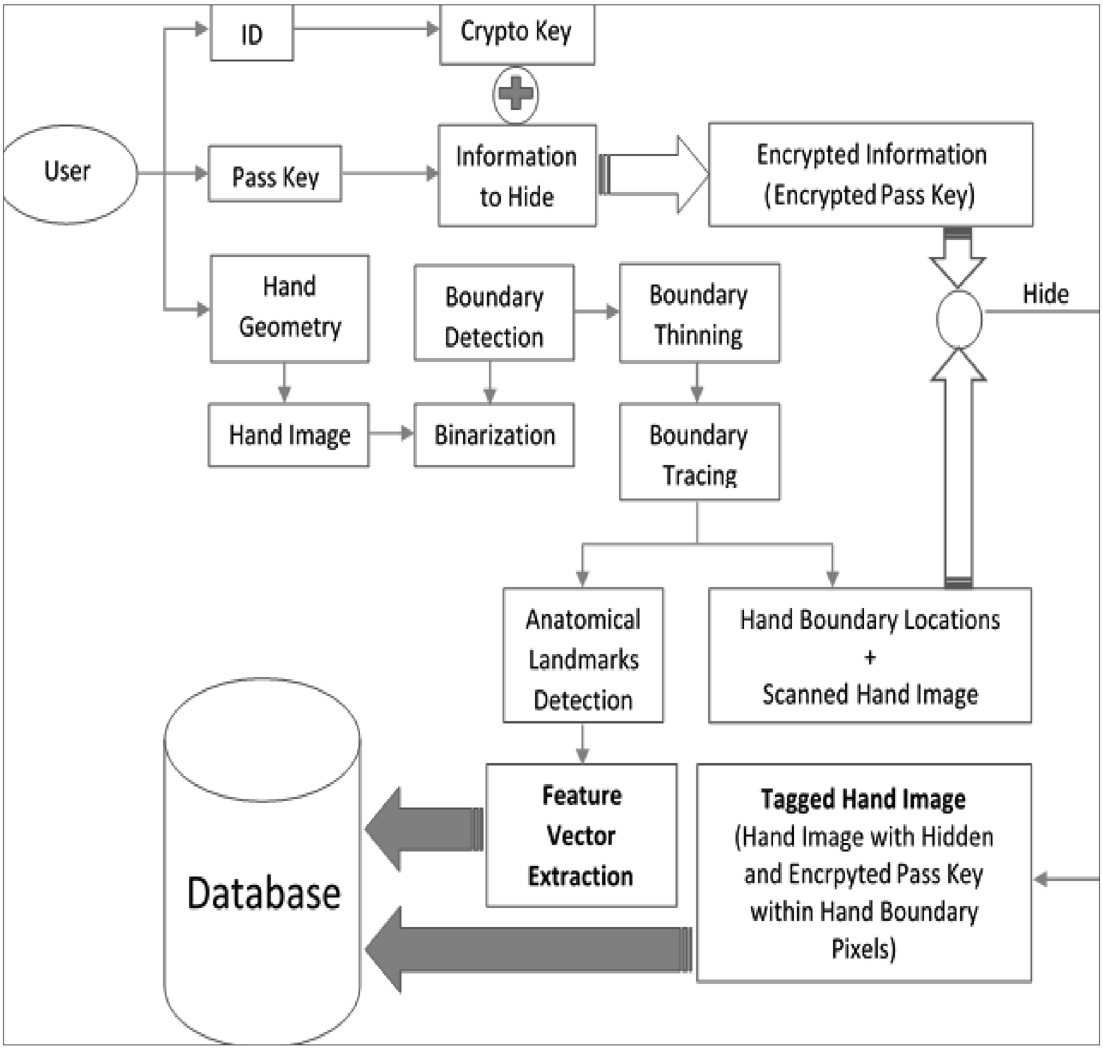
User's ID as Stego/Crypto key

=

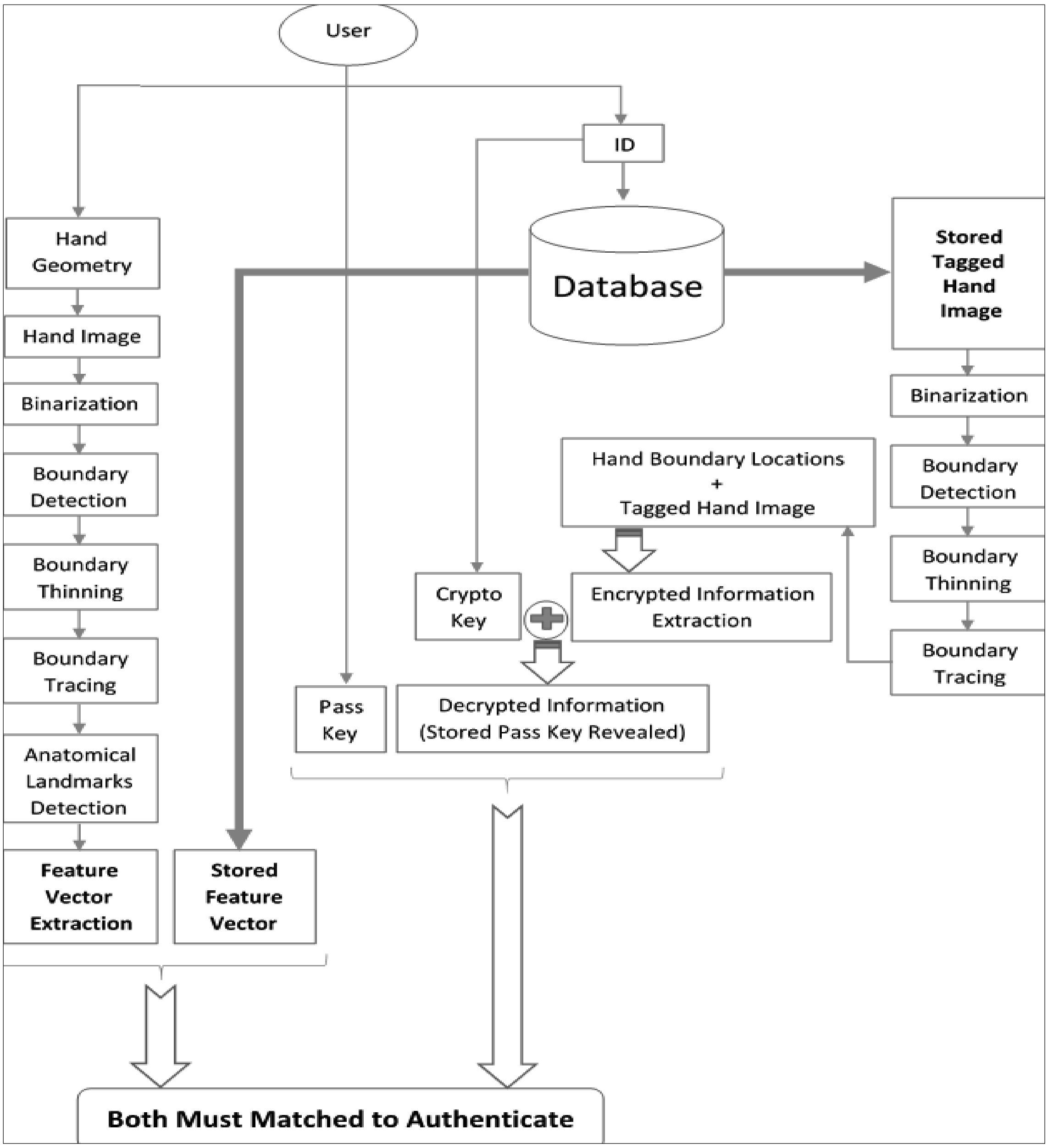
Tagged and Secured Biometric Hand Image

STEP BY STEP FUNCTIONING OF THE ALGORITHM

Enrollment Phase


ID
Crypto Key
User
Pass Key
Information to Hide
Encrypted Information (Encrypted Pass Key)
Hand Geometry
Boundary Detection
Boundary Thinning
Hide
Hand Image
Binarization
Boundary Tracing
Anatomical Landmarks Detection
Hand Boundary Locations + Scanned Hand Image
Database
Feature Vector Extraction
Tagged Hand Image (Hand Image with Hidden and Encrpyted Pass Key within Hand Boundary Pixels)

Authentication Phase



How to Apply Encrypted Steganography in Biometrics?

The pass key – which will be used to authenticate the user in conjunction with his biometric information which will be grabbed from the database using his ID – will be encrypted using the user's ID.

Pass Key ⊕ User's ID ➔ Encrypted Pass Key

This encrypted pass key will be hidden in the hand biometric image in some certain locations only (only the pixels that identify the borders of the hand image) using the least significant bit insertion technique.

Now to show how this becomes useful, you only need 8 bits to represent ASCII text and there are three extra in every pixel of the image. Therefore, with every three pixels, you could form one letter of ASCII text. This may not seem like a lot, but when the standard image size is 640 × 480 pixels, that add up to a lot in a hurry. In order to make this practical, after the user introduces his hand to the biometric capturing camera, and types his "ID Number" in the system and his "pass key" for authentication, the computer program will work in two parallel paths.

One will capture the hand image, and apply the pre-described processing steps to get a defined border of the user's hand, then find the anatomical hand marks, which will lead in turn to the feature vector that will be used in authentication phase.

On the other hand, the program will convert both "pass key" and "ID Number" to a binary, and encrypt the "pass key" using the "ID Number" to get an "encrypted pass key." Then using only the pixels that represent the border line of the user's hand (the locations in the hand image that we want to hide the "encrypted pass key" in) the program would go through every pixel and change the last digit to represent each letter of the "encrypted pass key" to generate a same looking hand image, but tagged with the "encrypted pass key," which will also be used latter in authentication phase.

In the authentication phase, to retrieve back the "pass key," the program will apply the same pre-described processing steps to the "tagged hand image" to retrieve border pixels of hand, then to go through every pixel that is labeled as hand border pixel, and take off the last digit and use that to form the pass key, but still encrypted.

So, to retrieve back the "pass key," the "encrypted pass key" will be decrypted using the user's ID.

Encrypted Pass Key ⊕ User's ID➔Stored Pass Key

This "stored pass key" will be compared with the "pass key" which the user gives while authenticating.

Also, the program will capture the user's hand, to extract a "real time feature vector," which will be compared with the "stored feature vector" in the database.

Both "biometric template" and "pass key" have to match with those stored in the database to authenticate this user otherwise he will be reported an intruder.

CONCLUSIONS

Although the efficiency of biometrics in identification of people is very accurate and highly secured, but still the data concerning it is not a secret, and if it is compromised, it would compromise the integrity of the system where protection is required.

Steganography has its place in security. There are an infinite number of steganography applications. This paper explores a tiny fraction of the art of steganography. It goes well beyond simply embedding text in an image.

However, detecting an embedded message defeats the primary goal of steganography, that of concealing the very existence of a hidden message. Hence, the secrecy of the stego-key is of vital importance for a successful steganographic process. There is always a challenge to build a fraud-resistant system, also there is always a challenge to breakthrough this system, and either is going to be the winner. The author hopes that it is the Security System.

REFERENCES

1. Jain AK, Bolle R, Pankanti S. (Eds). *Biometrics Personal Identification in Networked Society*. Kluwer Academic Publishers; 1999.
2. Sonka Milan, Hlavac Vaclav, Boyle Roger. *Image Processing, Analysis and Machine Vision*. Chapman & Hall; 1993.
3. Disappearing Cryptography. *Information Hiding: Steganography & Watermarking,* 3rd Edn. Peter Wayner, Elsevier; 2009.
4. Wikipedia: Steganography "http://en.wiki pedia.org/wiki/Steganography"
5. Nader A. Rahman. A prototype of automatic hand geometry verification system. *MSc. Thesis*. Systems and Biomedical Department, Faculty of Engineering, Cairo University, 2002.
6. Jang K, Chin T. One-pass parallel thinning: Analysis, properties, and quantitative evaluation. *IEEE Trans. on Pattern Analysis and Machine Intelligence*. Nov. 1992; 14(11).