International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

Digital Signature of Document using Human Palm

Murooj Mohammed Aboodn, Ziyad Tariq Mustafa Al-Ta'I, Naji MutarSahib

Abstract: ***A digital signature is a checksum which depends on the time period during which it was produced. Human palm biometric is one of the fastest, accurate, reliable and secure biometric techniques for identification and verification because it provides automatic authentication of an individual based on unique features in palm structure. In this paper, an efficient digital signature model for the document is proposed by using human palm. Human palm can give unique features which can be used in generating a secure digital signature. Therefore, this model consists of two sides: the embedding side and extracting side. The embedding side includes (1) image preprocessing stage:(color to grayscale and histogram equalization). (2) feature extraction stage:(GLCM (Haralick) algorithm). (3) Generating digital signature stage:(Elliptic Curve and Cubic Spline function with MD5 algorithm). While the extracting side contains extracting signature stage and matching stage. The accuracy of the generated digital signature by the proposed model is 100%, however false acceptance rate (FAR) is 0%, false reject rate (FRR) is 0%, and equal error rate (ERR) is 0%.***

Keywords: Digital Signature, Palm Print, Elliptic Curve and Cubic Spline function with the MD5 algorithm.

I. INTRODUCTION

Biometric systems are the most important systems used in our everyday life. Because of a lot of threats, fraud and identity theft, it is important to secure and maintain data accurately. But theft and impersonation still hinder data security by stealing passwords, PINs, and IDs. [1] A digital signature can be defined as a set of tests produced within a certain time period. This depends on all the bits of the message sent and on the secret key when checked it is not necessary to know the secret key. [2] The system of digital signature has been used in authentication, integrity, and approval of the transmitting digital data field among end-users. This system presents a technique for secured data during transmission by using different algorithms, which are divided into three main algorithms [3,4]: (1- key generation: this algorithm has two kinds symmetric and asymmetric, where the first kind has been used as a single key between the sender and receiver whereas the second kind is broken into public key and private key. 2- Signing: this algorithm generates the signature according to the data, message, and private key. Thus, the message will be sent with the digital signature to the receiver. 3- Signature verification: this algorithm is the last one, it has been executed in the receiver side to get on the transmitted data. The valid signature allows the receiver to read the received message and ensure its data.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

Murooj Mohammed Aboodn*, Professor, Department of Computer Science, University of Diyala, Baqubah, Iraq.

Ziyad Tariq Mustafa Al-Ta'I, Department of Computer Science, University of Diyala, Baqubah, Iraq.

Naji Mutar Sahib, Department of Computer Science, University of Diyala, Baqubah, Iraq.

II. RELATED WORKS

Related recent studies, which have proposed several algorithms on digital signature and palm print on texture feature, are discussed in this section: In 2014 M. Behera and V. K. Govindan [5], an approach was proposed using PCA (Principal Component Analysis) with the extraction of the reduced-dimension feature. This approximate proposal is excellent in terms of performance in accuracy and quality. PCA-based features reduce noise and memory usage. In 2016 K. Tamilsevan, et. al. [6] proposed a hybrid approach of using finger and palm vein for the design of the biometric system has been proposed. The proposed system approach simultaneously acquires the finger and palm vein database and combines these two pieces of evidence using a hybrid comparison strategy in order to increase the accuracy and sensitivity of the system while reducing the time complexity and harmfulness to a human being.

In 2017 J. A.Shaikh and U. D. Kolekar [], a system has been developed to identify the printing of palm-based on a gray text matrix feature. Using the Euclidean distance tool, the Harlick feature of the sub-images of each area of interest (ROI) was extracted to create a very small vector of features, however better accuracy is obtained, also there is an improvement on performance parameter, the False Acceptance Ratio (FAR) and False Rejection Ratio (FRR).
In 2017 K.J Archana, et. al. [8], through the focus of (ROI), which is very important in palm printing and based on (GLCM), a new algorithm was discussed to define palm printing. Compared to the recovery of (ROI) dynamic, the palm area of recognition is few when using fixed size (ROI). The proposed algorithm focused on the extraction of maximum possible ROI. Texture features are extracted using GLCM from dynamic ROI image. The experimentations are performed on the Poly U database to validate the proposed algorithm.

III. PALM PRINT

The definition of the palm as follows, our hand internal surface from the wrist to the fingers root. When we press on the surface an impression is made which is the print , while the print of the palm print can be said as the of the skin for the palm, comprised of the physical features of the skin designs like lines, texture , and points. The place that palm prints could exist is on the object surface , primarily because of the perspiration. When the hand has no water it led to less observable prints. The literature review shows there is two major part of the palm prints , forensic and non-forensic.

The forensic investigation is usually used in the actual palm prints that exist in the crime scene while the study of the non-forensic may use techniques of imaging to achieve noticeable human palm prints of a palm. Authentication of the Palm print is a method of the personal authentication that uses features of exceptional palm print , that may or may not be noticeable to the bare eye. The method that can be distinguished among two-person using the characteristic of the palm print by designing a suitable algorithm. Palm prints are rich in characteristic: principal lines, ridges , winkles , minutiae points and singular points , as display in Figure 1.1. Palm prints and fingertip are different in the surface area which the latter is much larger but are enclosed with the same type of skin of a finger [9].

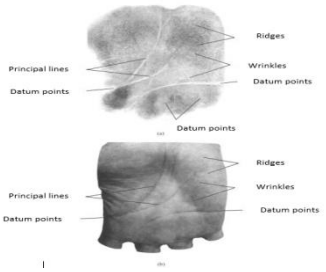


Fig.1: Different features of palm print (a) inked palmprint (b)inkedless palmprint [9]

IV. FEATURE EXTRACTION

The maximum related information is clearly represented if the features, objects of interest characteristics is selected sensibly so that the image has to suggestion for a complete characterization a lesion. methodologies of the extraction of the feature examine objects and images to excerpt the greatest prominent characteristics that are the representation of the object for the various classes. The input of the classifiers are Features that allocate them to the class that they represent [10]. Extraction of the feature is the image database indexing; mathematically, a vector of n-dimensional with its components calculated by certain analysis of the image is the representation of the feature. The three feature signifier primarily used most regularly throughout extraction of the feature are form, texture, and color [11].

A- Texture Features

One of the most significant features in the analysis of the image is texture. The texture is an attempt to analyze and quantify instinctive qualities defined by expressions like as silky, smooth, rough, or bumpy as a spatial variation role in pixel concentrations. The selection of the features of the texture should be as compressed as possible and at the same time discriminating as it could be. A set of features of the texture must be found with respectable power of discriminating. Texture features can be established by the methods such as Gabor Filter, Haar Wavelet Decomposition and Wavelet GLCM, etc. [12].

B- Features Extracted from GLCM

Haralick et al have projected several beneficial texture features that can be calculated from the co-occurrence, depending on the GLCM, numerous measures of texture feature are distinct. Like Energy, Entropy, Contrast, Inverse Difference Moment(IDM), Homogeneity, Mean. [13,14].

V. ELLIPTIC CURVE CRYPTOGRAPHY

Victor Miller was the introducer of the Elliptic Curve Cryptography (ECC),. In comparison to the other method such as RSA, The main attraction is that it provides security equally for a far with smaller key size, theory decreasing overhead of processing. ECC is depending on the problem of Discrete Logarithmic over the points on an elliptic curve [15]. ECC is a relative of discrete logarithm cryptography. The cartesian coordinate system is the definition of An elliptic curve E over Zp as in Figure 10 and an equation of the form [15]:

$y2 = x3 + ax + b$ ……1

where a, b ε Zp, and $4a3 + 27b2 \neq 0 \pmod p$, together with a special point O, called the point at infinity.

The set E(Zp) comprise of all points (x, y), x ε Zp, y ε Zp, that fulfill the defining equation, together with O.

every value of a and b offers a diverse elliptic curve. The point on the curve is the public key while the random number is the private key. The public key is gained by multiplying the private key with a generator point G in the curve[15].

VI. MD5 ALGORITHM

Message-Digest Algorithm 5 or MD. MD5 is encryption that considers non-reversible algorithm. It is generally applied in many features, including digital signature, information encryption in a database and communication information encryption. Before the private key is signed by digital signature soft, great amounts of information are compressed to a trusted format. A short explanation of MD5 algorithm as follows: MD5 algorithm split plaintext input into blocks and every that has 512- bit, and every block is also split into sixteen 32-bit message words, after a sequence of processing, the algorithm outputs contain four 32-bit message words After these four 32-bit message words are spilled, the algorithm generates a 128-bit hash value that is the essential ciphertext [16].

VII. INTERPOLATION

Schemes of Interpolation should model a function, among or afar the recognized points, by certain plausible functional form. In order to ensure estimated greater function classes that might ascend in practice, the form should be adequately broad. There is a wide mathematical literature that concern to theorems about what kind of function can be estimated. The job includes finding an estimated function to use in place of a more complex one. When the interpolation is used, you are given the function f at pa oint not of your own selecting. While the function approximation, you are allowable to calculate the function f at any wanted points for the goal of developing your approximation. The job , then, is to evaluation $f(x)$ for arbitrary x by, in some sense, sketch a smooth curve through the value of $f(x_i)$.

There are three cause for the interpolation $first$; methods of interpolation are the foundation, for many other processes like differentiation of the numerical, integration and methods of the solution for normal and equations of partial-differential.

*Second,*these approaches e s tablish some significant theory about polynomials and the numerical approaches accuracy *.third,* interpolating with polynomials helps as an excellent introduction to some techniques for drawing smooth curve. [17]

VIII. THE PROPOSED SYSTEM

The main goal of the proposed system is to develop a better-suggested system for digital signature of the document by using human palm as shown in Figure (2).

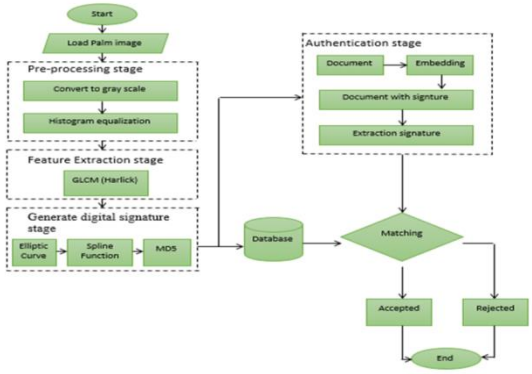


Fig.2: Flowchart of The Proposed System

Usually, the suggested model has some basic phases to implement all relevant produce signature and verification tasks. The general structure of the proposed system has five main stages. The first stage is the image preprocessing stage, the second stage is the feature extraction, while the third and the fourth stages are the generate digital signature and authentication stage, finally, the last stage is the matching stage

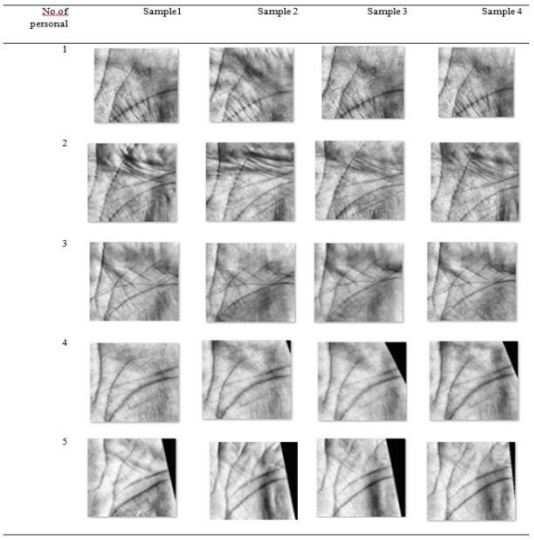


Fig 3Original Image of Palm data set

A- Palm Image Preprocessing Steps

The image preprocessing steps includes (RGB to Grayscale conversion, image enhancement (histogram equalization)) which can be used by the system

Step1: Loading Original Images

In this step, the number of loading original images are five as shown below in figure (3).

In this step, are used to convert the color format of the image from RGB to Grayscale. As shown in Figure (4).

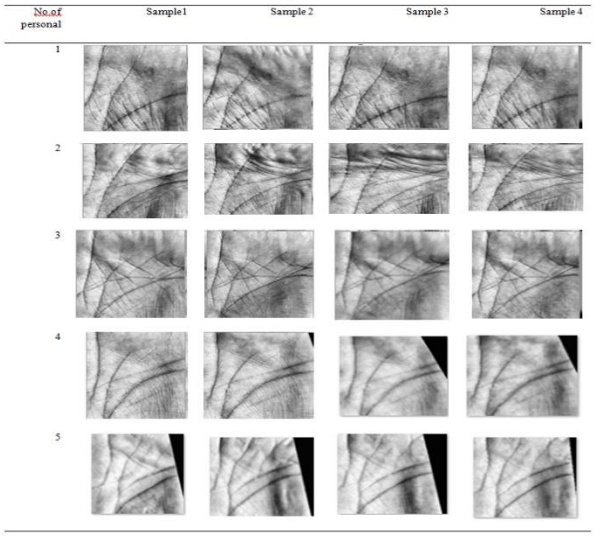


Fig.4 Examples of Image Conversation to Grayscale image

Step3: Enhancement with Histogram Equalization

In this step, Because most of the palm images have lows contrasts and also may have non-uniform brightness dues to the changes in lights sources positions, examples of palm enhancement results are presented in Figure 5.

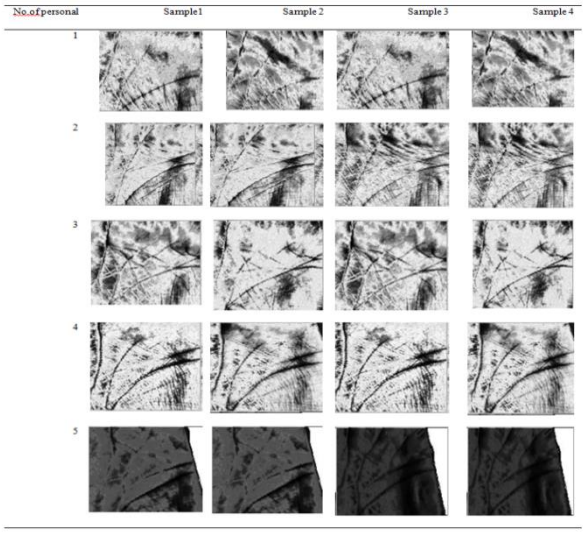


Fig.5: Enhancement with Histogram Equalization

B-Haralick Algorithm

In this stage, the intersection points are found in two stages as shown in table (1):

1. Cross the points between the samples.
2 - Cross the points between the Data Set.

Table (1): Haralick features

Personal	Sample1	Sample2	Sample3	Sample4	Intersection for all samples	Intersection for all data set
1						
2						
3						
4						
5						

In the table (2) shows the number of points and locations specified in the previous table.

Table (2): Find the intersection points of the database

The intersection of data set	No. of point	Coordinate point
	248	(0,129)_(0,132)_(0,133)_(4,14)_(14,4)_(38,68)_(51,79)_(68,38)_(68,80)_(68,133)_(73,102)_(,99).....
	169	(0,119)_(0,126)_(0,135)_(0,138)_(7,14)_(14,7)_(24,34)_(25,27)_(27,25)_(30,34)_(34,24)_(34,30)_(41,69)
	83	(0,140)_(15,23)_(23,15)_(23,29)_(29,23)_(29,29)_(29,33)_(33,29)_(67,80)_(76,76)_....
	14	0
	60	(0,5)_(1,3)_(1,6)_(3,1)_(3,8)_(4,6)_(5,0)_(6,1)_(6,4)_(6,6)_(6,9)_(6,11)_(6,14)_(8,3)_(8,21)_(8,24)_(9,6)_(10,13)_(11,6)_(11,21)_(11,24)_(12,18).....

C- Elliptical Curve

In this stage the is applied where all the points that belong to the Galois Field are extracted using (a, b, q) coefficient, which was selected for everyone in Data Set.

Table (3): Elliptical curve

Sample	Max x	Max y	prim	A	p	No. of point	Coordinate for all pint
1	127	127	127	0	132	1,11|77,71|6,92|37,117|62,14|101,109|38,1|30,14|72,78|118,36|46,38|.....	129
2	139	139	139	0	126	1,31|76,138|97,60|18,113|11,117|112,43|12,73|28,106|.....	163
3	127	127	127	15	23	0	20
4	0	0	0	0	0	1,8|11,1|20,3|5,10|0,4|15,5|2,7|21,12|13,8|9,15|17,1|6,10|.....	0
5	23	23	23	1	3	1,9|10,10|11,0|10,3|1,4|0,1|	30

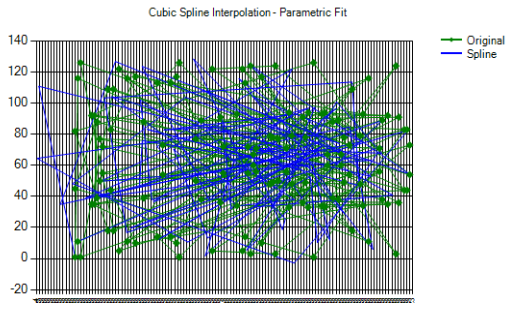
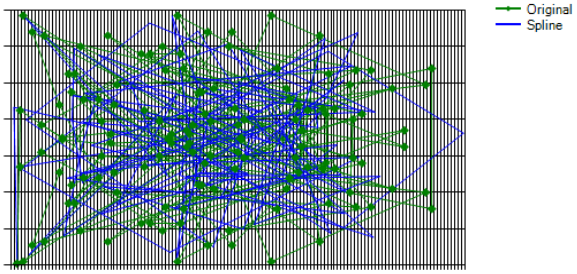
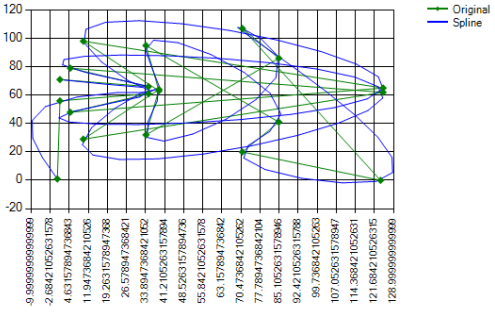
D- Spline function

After extracting points from an elliptic curve, this is considered a control point Through which coefficient (a, b) are obtained. In this step, using a cubic spline function to obtain values between the points (which are practically specific).

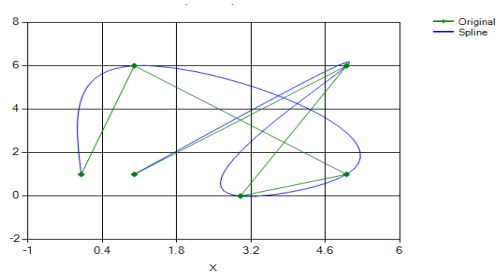
Table (4) Show spline function

person	No. of point	A	B
1	1,11|77,71|6,92|37,117|62,14|101,109|38,1|30,14|72,78|118,36|46,38|.....	16.76451,-0.7590468,2.928624,106.91,-99.08371,116.9296,-5.073877,17.49549,36.40501,-39.62466,1.591855,-18.35819,25.90898,-	16.76451,-0.7590468,2.928624,106.91,-99.08371,116.9296,-5.073877,17.49549,36.40501,...
2	1,31|76,138|97,60|18,113|11,117|112,43|12,73|28,106|.....	92.91501,29.268,-88.34368,0.743706,122.2114,-84.84505,3.279605,70.82192,-61.48873,116.4657,-21.32333,-11.14172,48.85456	17.84187,12.98322,-9.514316,-34.69373,-4.341859,0.3689356,72.81547,-10.82032,-26.51935,
3	0	-5.277642,-7.714694,69.25935,-45.66262,7.932518,20.29852,-109.9719,8.6695,147.9956,-41.28163,	-5.277642,-7.714694,69.25935,-45.66262,7.932518,20.29852,-109.9719,
4	1,8|11,1|20,3|5,10|0,4|15,5|2,7|21,12|13,8|9,15|17,1|6,10|.....	3.927491,3.18005,-1.305825,0.5278082,4.517166,.....	6.102664,10.4385,-4.938031,1.939002,-15.36695,23.54535,-0.6631657,-2.310248,
5	1,9|10,10|11,0|10,3|1,4|0,1|	2.375535,-3.698605,2.572632,2.365764,-10.15821,0.9293934,-1.456154,-0.7112004,.....	4.501919,1.117156,-1.615244,8.358788,0.6003506

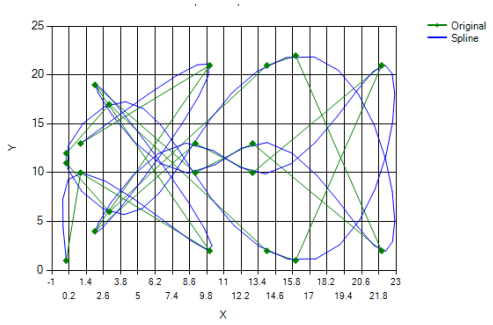
Table (5) Graph the cubic spline curve

person	Cubic spline function
1	
2	
3	

4



5



E- MD5

In this stage, The digital signature is being extracted through coefficient (a, b) for Everyone in Dataset, where the algorithm is applied MD5 For this coefficient and extract a digital signature for coefficient (a,).

Table(6)MD5 algorithm

Personal	Massage coefficient A	Massage coefficient b
1	16.76451,-0.7590468,2.928624,106.91,-99.08371, 116.9296,-5.073877,17.49549,36.40501,-39.62466, 1.591855,-18.35819,.....	33.529,-30.92391,23.53088,-98.78519, 87.66576,-172.9238,-3.250352,70.87595,- 9.462164,-5.267771,-28.55753,89.3567,- 42.60853,.....
2	92.91501,29.268,-88.34368,0.743706,122.2114,- 84.84505,3.279605,70.82192,-61.48873,116.4657, -21.32333,-11.14172,.....	185.83,-47.9892,-2.973895,0.895619,- 8.225797,-73.2796,14.1744,-13.43102, 13.41602,88.74588,-48.46449,-0.9984154, 3.403606,.....
3	-5.277642,-7.714694,69.25935,-45.66262, 7.932518,20.29852,-109.9719,8.6695,147.9956,- 41.28163,-2.606987,22.3963,.....	-10.55528,-1.097977,62.68635,-146.0061, 51.42171,-7.593447,-33.31564,12.33483,- 62.141,-21.28272,-4.959132,.....
4	3.927491,3.18005,-1.305825,0.5278082, 4.517166,.....	7.854982,-5.134997,-0.9303941,5.606321, 2.258583,.....
5	-2.375535,-3.698605,2.572632,2.365764,- 10.15821,0.9293934,1.456154,-0.7112004,- 3.860729,20.27983,-16.25956,8.068276,....	-4.751069,-3.331698,14.70235,-1.242035,- 2.348181,-2.322185,15.34856,-7.482711, 3.860083,-5.763913,-7.806979,.....

F- Tests

The false acceptance rate (FAR), is the measure of the likelihood that the security system will incorrectly accept the digital signature.

FAR= number of false acceptances/ number of identification attempts.The false recognition rate (FRR), is the measure of the likelihood that the security system will incorrectly the digital signature.

FRR= number of false recognitions / number of identification attempts.

The equal error rate (ERR) is the intersection of FAR and FRR. While accuracy is:

Accuracy= 1- ERR. (1)

The tests results are shown in table (4. 8).

Table (7) The Tests Results

No. of attempts	FAR	FRR	ERR	Accuracy
100	0	0	0	100

IX. CONCLUSIONS

Several conclusions have been deduced from the obtained results of the proposed model, such as:

1. Figures (1.2 and 1.3) prove that the preprocessing stage in the proposed model gave accurate results that made palm images more distinguishable.
2. Tables (1-1 and 1-2) describe that the GLCM (Haralick) algorithm can extract important features from palm images.
3. Table (1-3) indicates that elliptic curve points can be used as good control points for cubic spline curves.
4. Table (1-4) shows the good choice of in-between points for spline curves. While table (1-5) clarifies the spline curves.
5. Table (1-6) describes the values of the coefficients after applying the MD5 algorithm which can be used as a signature in the embedding stage and can be used in the matching step at extracting stage.

The possible future works for digital signature take several directions including:

- Adapting the proposed model for a large-scale iris database to make the system more reliable.

The digital signature of the document by using the human brain.

REFERENCES

1. Basu and Mita, "Development of a human identification system from finger vein biometric," Digital Library, 2013.
2. M. N. Nabi, S. Mahmud and M. L. Rahman, "Implementation and Performance Analysis of Elliptic Curve Digital Signature Algorithm," Daffodil International University Journal of Science and Technology, Vol:2 (1), 2007.
3. Luxton David D., R. A. Kayl, and M.C. Mishkind. "MHealth data security: The need for HIPAA-compliant standardization," Telemedicine and e-Health, Vol: 18 (4), PP:284-288, 2012.
4. Stallings, William, "Cryptography and Network Security, 4/E," Pearson Education India, 2006.
5. M. Behera and V.K. Govindan, " Palmprint Authentication Using PCA Technique," (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3), PP: 3638-3640, 2014.
6. K. Tamilselvan, R. Krishnaraj, P. Sukumar, T. Jayakumar, "Security Method for Human Finger and Palm Image Identification," International Journal of Emerging Technologies in Engineering Research (IJETER), Vol: 4 (6), 2016.
7. J. A. Shaikh, U. D. Kolekar "Palm Print Recognition Using Textural Harlick Feature," International Journal of Applied Engineering Research, Vol: 12, (11), pp. 2922-2925, 2017.
8. K.J Archana, V.S Sangeetha, and Y. L. Malathi Latha, "Palmprint Identification based on texture features using GLCM through Dynamic ROI," International Journal of Computer Science and Engineering - (ICRTESTM) - Special Issue – April 2017.
9. D. D. ZHANG, PALMPRINT AUTHENTICATION, United States of America: Springer, 2004.
10. A. K. Mohanty et al., "Image Mining for Mammogram Classification by Association Rule Using Statistical and GLCM Features" Journal: International Journal of Computer Science Issues ISSN: 16940784, 2011.
11. I. N. Ibraheem," Color Models Indexing for Content-Based Image Retrieval System", Ph.D. Thesis, Department of Computer Science, University of Technology, IRAQ, 2009.
12. A. Tiwari, A. K. Goswami and M. Saraswat, "Feature Extraction for Object Recognition and Image Classification," International Journal of Engineering Research & Technology, vol. 2, no. 10, pp. 1238-1246, 2013.

13. T. Ojala, M. Pietikaine," Texture Classification", M.Sc thesis, Machine Vision and Media Processing Unit, University of Oulu, Finland, 2010.
14. P. Mohanaiah, P. Sathyanarayana and L. GuruKumar, "Image Texture Feature Extraction Using GLCM Approach," *International Journal of Scientific and Research Publications*, vol. 3, no. 5, pp. 1-5, 2013.
15. Thangarasu.N and A. L. Selvakumar, "Implementation and Secured Authentication Key using Elliptic Curve Cryptography," International Journal of Innovative Research in Information Security (IJIRIS), vol. 1, no. 2, pp. 66-71, 2014.
16. A. K. Kashgar and M. K. Dhariwal, "A Review Paper of Message Digest 5 (MD5)," *International Journal of Modern Engineering & Management Research*, vol. 1, no. 4, pp. 29-35, 2013.
17. A. H. Fadel, S.B.Sadlkhan, "Modified Digital Signature Based on Cubic Spain Function," M.S.C University of Babylon, 2013.