Online Multi-Parameter 3D Signature Verification through Curve Fitting

P. M. Rubesh Anand[1], Gaurav Bajpai[2] and Vidhyacharan Bhaskar[1]

[1] Department of Electronics and Communication Engineering, SRM University, Kattankulathur – 603203, India
[2]Faculty of Engineering, Kigali Institute of Science and Technology, B.P. 3900, Kigali, Rwanda

Summary
Biometric based personal identification is a reliable and widely accepted method for authentication. Human 3D signature is distinct from other biometric authentication methods due to the presence of third dimensional hidden information. In this paper, a new model for on-line 3D signature verification using multiple parameters is proposed. The parameters considered from human signature namely, velocity, acceleration, pressure, direction, pen ups/downs, total time taken, length and depth of the signature are unique for each person. The proposed model highlights the third dimensional distinctive parameter, depth of the signature for its hidden information. Curve fitting is performed on the points obtained from different non-linearly spaced layers of the signature pad. The best fitted curves from all the layers and other signature parameters are used in the process of verification of 3D signature. The digital multi-parameters of the 3D signature are further encrypted with cryptographic algorithms to protect from cryptanalysis. The attempts for 3D signature expert forgery by satisfying both the global and local parameters of the signature are difficult. The application of the 3D signature verification broadly ranges from authentication of financial transactions to authorization of administrative documents.

Key words:
3D Signature verification, Authentication, Biometric Security, Curve fitting, Forgery prevention

1. Introduction

The rapid growth of internet has lead to numerous on-line business transactions and administrative works through computers. The need to ensure that only the right person gets access to the highly secured information, the requirement for reliably effective security methods to protect the information transferred through insecure channel leads to various authentication mechanisms [1], [2]. The term biometrics refers to individual recognition based on person's unique characteristics. In the biometric techniques, the individual is identified by his/her physiological or behavioural characteristics. The physiological identification is based on the biological individuality of users, like, fingerprint, face, hand geometry, vein patterns, retina and iris. The behavioural biometric identification considers voice or handwritten signature [3]. Although physiological biometrics have consequently become more integrated into commercial products, behavioural biometrics exhibit the quality of memory that make them attractive for security applications. The techniques used for authentication in computer systems, like, token based, knowledge based identity verification requires the possession of token, remembering of the password/pass phrase are prone to be forgotten, disclosed or compromised. In contrast to the knowledge or token based verification techniques, the biometric based identification/verification offers the advantage of presenting the individual personality, whose attributes are hard to steal or forge [4].

Human hand written signature is used as a traditional way of authentication in business and financial transactions due to its unique nature of individuality. The static and dynamic signature verification for the paper-based documents and transactions are done by humans. The challenges faced in that verification are: any signature can be learnt; it can be changed by the owner and has several versions of the signature depending on the level of importance or intent of the signer [5]. Most humans are a relatively poor judge of handwritten signature authenticity leading to the success of the expert forgers. Presently, the writing pad with dedicated pen for 2D handwriting recognition is available for email signing and handwriting recognition [6], [7]. The 2D signature verification methods are vulnerable to spoof [8], [9]. The main reason for the failure is due to the fact that signatures are verified in 2D. This paper proposes a new model for reliable and accurate identification/verification of 3D hand written signature by considering the depth parameter in different layers of z-axis in the signature pad to enhance secure transactions. Signature verification has a number of statistical features that can be derived from the basic set of data from the signature pad. This paper uses only the parameters which have more uniqueness like velocity, acceleration, pressure, direction, pen ups/downs, total time taken, length of the signature. Apart from these parameters, the hidden parameters like depth of the signature, curve fitting, surface fitting and solid angle are calculated by the mathematical functions. The application of this proposed

Manuscript received May 5, 2009
Manuscript revised May 20, 2009

model of 3D signature verification is for the authentication of on-line financial transactions and documents. The paper-based signature authentication and authorization can be replaced by 3D signature verification if e-governance is fully implemented.

Further, this paper is organised into six sections. Section 2 covers the introduction to human signature parameters, section 3 describes about the proposed model, section 4 explains the authentication algorithm, section 5 shows the necessity of encryption, section 6 highlights the advantages along with applications of the proposed model and section 7 presents the conclusion.

2. Parameters of Interest

The handwriting recognition and signature verification studies often make use of nearly 50 features [10], [11]. The features considered in many of those work like velocity, acceleration, pressure, direction, pen ups/downs, total time taken, length of the signature for the verification of signature is categorized as time based feature or global parameters [12], [13]. Local parameters concern features extracted from specific parts of the signature. The depth of the signature, process of curve fitting, surface fitting, calculation of solid angles are considered as local parameters. Global parameters are denoted as $\{G_i\}$ and local parameters are denoted as $\{L_i\}$ where, $i = 1,2,...,k$ depending upon the number of parameters (k) considered.

Global parameters considered in the signature verification using 2D values in time axis are commonly reported in the field as:

(a) ***Velocity:*** The rate of change of displacement along the x - axis during the process of signing.

(b) ***Acceleration:*** The rate of change of velocity occurring in the process of signing.

(c) ***Pressure:*** The stress level applied normally by the individual on the signature pad by the pen while signing.

(d) ***Direction:*** The pen movements in the x, y axis of the pad during the time interval of signing.

(e) ***Pen ups/downs:*** The total number of pen lifts during the process of signing.

(f) ***Total time taken:*** The time used between the initial point and the final point of the signature.

(g) ***Length:*** The full length of the signature is the same for an individual even if scaling is required.

This paper mainly deals with the local parameters which consider the 3D values as given below:

(h) ***Depth:*** This z axis parameter is the third dimensional value as points over the planes.

(i) ***Curve fitting:*** 2D curve fitting is performed by using the distinguished pressure points of the layers with polynomial curves used for the exact fit.

(j) ***Surface fitting:*** 3D surface fitting is performed with the points from different layers. The values of the best fit are used as the local parameter.

(k) ***Solid angle:*** The z axis values combined with the surface fitting is used to calculate the different solid angles between points and 3D surfaces.

3. Proposed Model

The existing models of biometric authentication are weak if cryptanalysis is performed on the transmitted data [14], [15]. The way to overcome this problem is to use hidden parameter along with strong cryptographic algorithm. In this paper, a model to bridge the gap between biometric

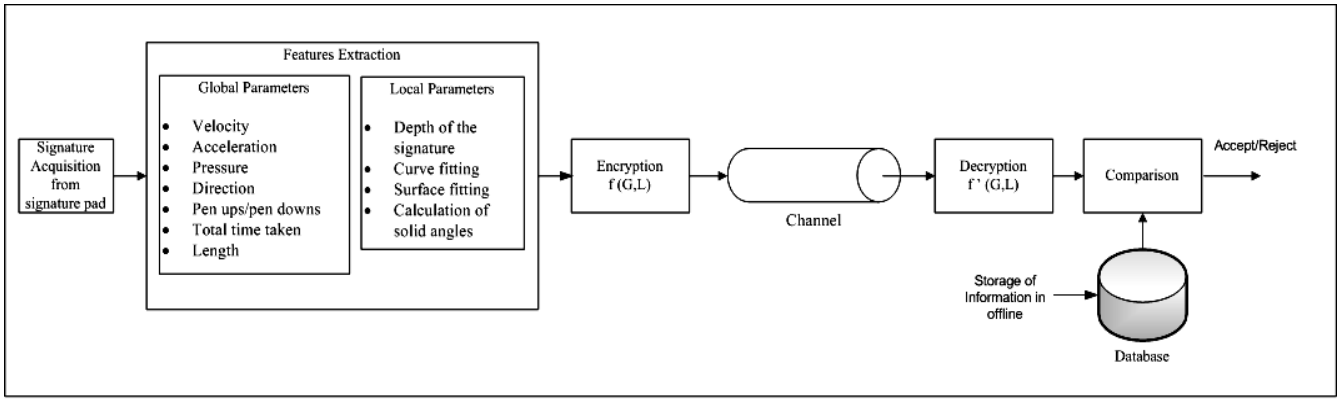

Fig. 1 Block diagram of the proposed model

authentication and security is proposed. The process of

authentication is performed with the global and local parameters. The 3D values of the signature are taken as the important local parameter of consideration in the proposed model given in Fig. 1. Encryption function is employed on the combined global and local parameters making individual parameter cryptanalysis a difficult process.

The model proposes a special signature pad with no need for any special type of pen to be used. As the individuals feel uneasy with different pen sizes, the model considers the use of all type of pens giving the freedom for their own choice of pen. The z-axis pressure variation is measured by non-linearly spaced layers of the signature pad as in Fig. 2.

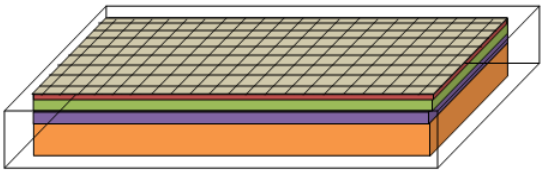

Fig. 2 Non-linearly spaced layers in the proposed signature pad

The non-linearity is considered in the model for the reason of minute pressure variation in z-axis remains with the upper layers. The spacing difference is small in the upper layers to record the minor variation of the depth of the signature. The lower layers are widely spaced to record the details of the heavy pressure points during the process of signing. This makes the signature to be three dimensional with depth. The signature pad has grid lines on its upper layer to help the individual in maintaining their usual angle of signing.

3.1 Data Acquisition

The data acquisition in the proposed dynamic signature verification system uses online acquisition by generating the electronic signals representative of the signature during the process of signing. The signature is sampled online for every interval of time to acquire the required data and extract the feature from it. The features extracted from the signature are denoted depending upon the global or local parameters as $\{\overrightarrow{G_1}, \overrightarrow{G_2}, \overrightarrow{G_3}, \overrightarrow{G_4}, \overrightarrow{G_5}, \overrightarrow{G_6}\}$ or $\{L_1, L_2, L_3, L_4\}$. In the process of sampling, for the sampling period Δt, the sampled signal value from each layer $(1 \le l \le L)$ of the signature pad $S_l(n)$ at time $n\Delta t$ of the signing process $(0 \le n \le N)$ is given as,

$$\{S_l(n)\}_{n=0,1,2,\ldots,N} \quad (1)$$

(a) ***Velocity*** ***(*** $\overrightarrow{G_1}$ ***):*** The rate of change of displacement along the x - axis through the grid lines through sampling process is given as,

$$\overrightarrow{G_1} = \vec{v} = \frac{d\vec{x}}{dt} \quad (2)$$

(b) ***Acceleration*** ***(*** $\overrightarrow{G_2}$ ***):*** The rate of change of velocity calculated from the equation (2) as,

$$\overrightarrow{G_2} = \vec{a} = \frac{d\vec{v}}{dt} \quad (3)$$

(c) ***Pressure (*** $\overrightarrow{G_3}$ ***):*** The stress level applied on the pad by the pen, *F* being the force applied on the area *A*. Here, pixel is considered for the area *A*.

$$\overrightarrow{G_3} = \vec{P} = \frac{d\vec{F}}{dA} \quad (4)$$

(d) ***Direction (*** $\overrightarrow{G_4}$ ***):*** The pen movements in the *x*, *y* axis is recorded as binary value of 0 or 1 depending upon the backward or forward movement.

$$\overrightarrow{G_4} = \vec{x}, \vec{y} \quad (5)$$

(e) ***Pen ups/downs*** ***(*** $\overrightarrow{G_5}$ ***):*** The discrete signals $x(t)$ and $y(t)$ specify the location of the pen on the grid lines of the signature pad at time *t*, and the binary signal $u(t)$ specifies whether the pen is up or down at time t.

$$\overrightarrow{G_5} = \vec{u}(t) \quad (6)$$

(f) ***Length*** ***(*** G_7 ***):*** Mahalanobis distance function $d(\vec{x}, \vec{y})$ is used to determine the length of the signature as the function [16] is scale-invariant with the covariance matrix *S*.

$$\overrightarrow{G_6} = d(\vec{x}, \vec{y}) = \sqrt{(\vec{x} - \vec{y})^T S^{-1} (\vec{x} - \vec{y})} \quad (7)$$

3.2 Depth Analysis

The pressure applied on the signature pad during the process of signing leads to the formation of deep points in the different layers which are sampled at regular intervals. As the process of sampling is done on each layer for every interval of time, the locations of pressure points are obtained from the grids in each layer separately.

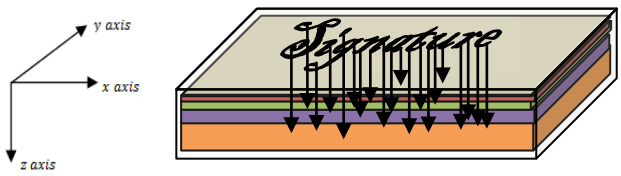

Fig. 3 Three-axis variations in the signature.

The three-axis variations are shown in Fig. 3 as x-axis for the left to right direction, y-axis for the top to bottom direction and z-axis for the depth of the signature (L_1). Fig.4 demonstrates the different pressure points on each layer.

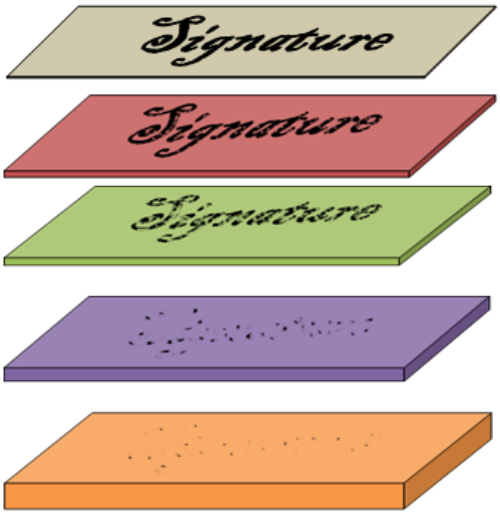

Fig. 4 The pressure points of the signature in each layer.

3.3 Curve Fitting

Each layer in the signature pad is considered as a 2D plane. The distinguished pressure points are produced by different levels of pressure applied over the layer in the process of handwritten signature. Those pressure points in each layer are considered with the curve fitting equation for a best fit of curve. The linear equations, polynomials, rational, logarithmic, exponential functions, non-linear transition, non-linear power functions are used for curve fitting. Apart from these equations and functions, there exist huge numbers of user defined functions giving a wide range of randomness. The fitted curve is a unique parameter which is hidden even from the owner of the signature.

$$f(x,y,z) = x^0y^0z^0 + x^1y^1z^1 + x^2y^2z^2 + \ldots + x^ny^nz^n \quad (8)$$

The distinguished points selected are matched by one of the way with the polynomial given in equation (8) to get the best fit of the curve. Once the curve is fit, the degree of the polynomial used to obtain the best fit of the curve is the local parameter (L_2). The distances between pressure points in each layer are calculated for signature verification. The distance between any two points (x_i, y_i, z_i) to (x_j, y_j, z_j) in different layers are given by equation (9).

$$\Delta P_{ij} = |P_i - P_j| = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (z_i - z_j)^2} \quad (9)$$

The effect of scaling due to the individual's signing condition is overcome by using the modulus ratio of point differences. The value ΔP_{ij} is normally equal and it is compared to that stored in the database during verification. This feature helps in effective verification of 3D signature of different sizes. Equation (10) shows the rate of change of x, y axis pressure point values with respect to time. This calculates acceleration between various selected points over the layers in the signature pad as,

$$\Delta R_t = \sum_{t=0}^{k} \left| \frac{\Delta P_i}{\Delta P_j} \right| \quad (10)$$

3.4 Surface Fitting

The pressure points from more than one layer are considered to fit a 3D surface. There exists many surface fits depending on the points considered in each layer. The optimum equation to describe the three dimensional empirical data is obtained from the best fit through the standard least squares minimization. The points between two, three, four and five layers are used to perform the best 3D surface fit. Various points of x, y, z axis from all the layers produce complex 3D surface. The fitted 3D surfaces is another unique local parameter (L_3) for verification. The 3D surface fitting utilizes the linear equations, polynomials, rational, logarithmic, exponential functions, linear regression, logistic functions, Fourier approximation, B-splines, parametric curves least squares approximations and user defined functions for 3D surface fitting. A 2D contour plot on the top and bottom of the surface fit graph is also a distinct value for (L_3).

3.5 Solid Angle

The points and surfaces in three-dimensional space produces the solid angle at every different point and location considered [17].

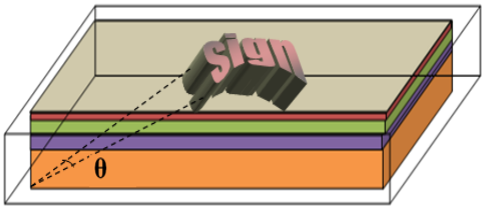

Fig. 5 The solid angle calculation in one of the layers.

This is a measure of scaling for the signature. The angle θ will remain constant for different sizes of the signature, making the process of verification unchanged. The fig. 5 exhibit the solid angle calculation in one of the layers. This hidden parameter (L_4) is important and effective data for 3D signature verification.

4. Authentication Algorithm

The authentication algorithm for the proposed model has two phases, namely, enrollment phase and verification phase. Enrollment phase works in offline and verification phase works in online.

4.1 Enrollment phase

During the enrollment phase, each legitimate individual is allowed to sign in the signature pad for registering the signature samples. Once the first sample is obtained from the signature pad, the features are extracted from it and the values are stored in the database. The features are extracted from all the possible combinations of global $\{\overrightarrow{G_1}, \overrightarrow{G_2}, \overrightarrow{G_3}, \overrightarrow{G_4}, \overrightarrow{G_5}, \overrightarrow{G_6}\}$ parameters as in the equations (11), (12) of $\overrightarrow{R_i}$ for i=1,2,…,k, k being the total number of combinations.

$$\overrightarrow{R_1} = \overrightarrow{G_1} + \overrightarrow{G_2} + \overrightarrow{G_3} + \overrightarrow{G_4} + \overrightarrow{G_5} + \overrightarrow{G_6} \qquad (11)$$

$$\overrightarrow{R_2} = \overrightarrow{G_2} + \overrightarrow{G_4} + \overrightarrow{G_5} + \overrightarrow{G_6} \qquad (12)$$

The local parameter features are extracted from $\{L_1, L_2, L_3, L_4\}$ and stored in the database individually. When the second sample of the signature is received, the extracted features are verified offline with the previous sample for variations. The degree of variance is calculated and stored. Once the enrollment of the 3D signature is completed after collecting sufficient number of samples, the full degree of variance from the complete set of signatures is calculated in order to minimize the False Acceptance Rate (FAR) and False Rejection Rate (FRR).

4.2 Verification Phase

During the verification phase, the signature is acquired from the signature pad and the features are extracted. The 2D curve fitting, 3D surface fitting and solid angle calculation leads to different unique values for individual signature. The best fit for every selected point is obtained by the algorithm. From the extracted features, the algorithm selects some combination of the global parameters along with the calculated local parameters. The selected parameters are sent through the channel after encryption for the process of verification. In order to combat from the Naïve, static and dynamic expert forgery, the local parameters of curve fitting, surface fitting and solid angle calculations are varied in the verification phase every time by the defined algorithm. The comparison of the received signature with the database determines whether the values fall within a certain statistical range and accordingly accept/reject is sent as the result of verification. The signature verification system is updated with the individual's more recent sample of the signature to avoid the minor variations in the signature of the individual due to aging or other known factors. The updated information is analyzed for modifying the authentication algorithm to be used.

5. Encryption

The attacks like Man-in-the-middle attack, cipher-text alone attack, exploit the security in the signature verification [18], [19]. The algorithm used for signature verification is time-dependent to avoid any attempt of cryptanalysis during the process of verification of signature. The encryption with strong cryptographic algorithms like symmetric, asymmetric key encryptions helps to make complexity in cryptanalysis. The selected parameters from the algorithm are combined with function $f(G, L)$ and encryption is preformed using XOR operation as given in equation (13). The function varies the combination of the considered global and local parameters every time along with different key k.

$$f'(G,L) = f(G,L) \oplus k \quad (13)$$

The encrypted data is sent for verification through the channel. The receiver decrypts the data as in equation (14) to get the features for verification from the database.

$$f(G,L) = f'(G,L) \oplus k \quad (14)$$

Each layer is encrypted with dynamic symmetric keys [20] and the whole signature is encrypted with asymmetric key to protect from spoofing and cryptanalysis. The database storing the detailed analysis of all the parameters is updated periodically and encrypted for higher protection.

6. Advantages and Applications

The physiological biometric authentication methods like fingerprint, iris, voice, face recognition can be spoofed by a duplicate or when the person is in unconscious state of mind [21], [22]. The behavioral biometric authentication like voice, handwritten signature possess strong barrier for such spoofing even when the individual is in medicated state due to the need for memory. Compared to voice, signature is widely accepted for the purpose of authentication due to the larger range of variations [23]. Theoretically, the 3D signature possess less FAR compared to 2D signature providing high security from forgery. These properties allow 3D signature verification to be deployed in the field of financial transactions, business contracts and administrative works through internet. The token based, knowledge based authentication methods can be replaced with 3D signature authentication for email login, credit card authentication, network administration, personal security for portable devices like laptops, palmtops. This makes the paper-based hand written signature authentication to be replaced by 3D signatures for the powerful and trust worthy implementation of e-governance. The authorization of the governmental orders, legal documents, tax documents, appointment letters, consent forms, visa applications and judiciary documents can be handled through online with the 3D signature verification.

7. Conclusion

The rapid growth of the internet leads to the increasing security requirements for the development of e-society. The on-line verification of signatures for authentication is needed for achieving fast and secure economical growth. The proposed model uses a customary personal authentication method that is accepted at both legal and social levels. The deployment of 3D signature verification can replace the present methods of authentications like token or password. The current need for a powerful authentication method in high security transactions like, banking and business can be satisfied by the wide range of security applications provided by the 3D signature authentication model. The verification database can be managed by banks, trusted third party or government for reliable and non-transferable authentication.

References

[1] A. Kholmatov and B. Yanikoglu, "Biometric authentication using online signatures," Computer and Information Sciences - ISCIS 2004, 19th International Symposium, ser. LNCS. Springer, pp. 373–380, October 2004.

[2] G. Dimauro, S. Impedovo, and G. Pirlo, "Algorithms for automatic signature verification," Handbook of Character Recognition and Document Image Analysis, H. Bunke and P. S. P. Wang, Eds. Singapore: World Scientific, pp. 605–621, 1997.

[3] K. W. Boyer, V. Govindaraju, and N. K. Ratha, Eds., "Introduction to the special issue on recent advances in biometric systems," IEEE Transactions on Systems, Man, and Cybernetics, vol. 37, no. 5, pp. 1091–1095, Oct. 2007.

[4] M. C. Fairhurst, "Signature verification revisited: promoting practical exploitation of biometric technology," Electronics & Communication Engineering Journal, vol. 9, no. 6, pp. 273–280, December 1997.

[5] S. J. Elliott and A. R. Hunt, "The challenges of forgeries and perception of dynamic signature verification," Proceedings of the 6th International Conference on Recent Advances in Soft Computing (RASC 2006), pp. 455-459, 2006.

[6] Intuos Pen Tablets, Wacom, [Online]. Available: http://www.wacom.com/intuos/index.php

[7] Interlink Electronics, eSign, [Online] Available: http://www.interlinkelectronics.com/esign/index.html

[8] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," Pattern Recognition, vol. 35, no. 12, pp. 2963–2972, 2002.

[9] L. Lee, T. Berger, and E. Aviczer, "Reliable on-line human signature verification systems," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 18, no. 6, pp. 643–647, June 1996.

[10] W. Nelson and E. Kishon, "Use of dynamic features for signature verification," Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, pp. 1504–1510, October 1991.

[11] D. Sakamoto, T. Ohishi, Y. Komiya, H. Morita, and T. Matsumoto, "Online signature verification algorithm incorporating pen position, pen pressure and pen inclination trajectories," Proceedings of IEEE International Conference on Acoustics, Speech, Signal Processing (ICASSP 2001), vol. 2, pp. 993–996, 2001.

[12] H. D. Crane and J. S. Ostrem, "Automatic signature verification system using a three-axis force-sensitive pen,"

IEEE Transactions on Systems, Man, and Cybernetics, vol. SMC-13, no. 3, pp. 329–337, May/Jun. 1983.
[13] B. Fang, C. H. Leung, Y. Y. Tang, K. W. Tse, P. C. K. Kwok, and Y. K. Wong, "Offline signature verification by the tracking of feature and stroke positions," Pattern Recognition, vol. 36, no. 1, pp. 91–101, Elsevier, Jan. 2003.
[14] A. I. Al-Shoshan, "Handwritten signature verification using image invariant and dynamic features," Proceedings of third International Conference on Computer Graphics, Imaging and Visualization (CGIV 2006), pp. 173–176, 2006.
[15] M. Zou, J. Tong, C. Liu, and Z. Lou, "On-line signature verification using local shape analysis," Proceedings of 7th International Conference on Document Analysis and Recognition (ICDAR-7), vol. 1, Edinburgh, U.K., pp. 314–318, Aug. 2003.
[16] R. Martens and L. Claesen, "On-line signature verification: discrimination emphasised**,"** Proceedings of the Fourth International Conference on Document Analysis and Recognition, Germany, pp. 657-660, 1997.
[17] P. M. Rubesh Anand, G. Bajpai, Vidhyacharan Bhaskar, and Sam M. Job, "Detection of the Malarial Parasite infected blood images by 3-D analysis of the cell curved surface," Proceedings of the 4th Kuala Lumpur International Conference on Biomedical Engineering (Biomed 2008), Malaysia, pp. 166-169, June 2008.
[18] Y. W. Kuan, A. Goh, D. Ngo, and A. Teoh, "Cryptographic keys from dynamic hand-signatures with biometric security preservation and replaceability," Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies. Los Alamitos, CA: IEEE Computer Society, pp. 27–32, 2005.
[19] Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," Second Edition, John Wiley & Sons, 1996.
[20] P. M. Rubesh Anand, Gaurav Bajpai and Vidhyacharan Bhaskar, "Real-Time Symmetric Cryptography using Quaternion Julia Set," International Journal of Computer Science and Network Security, vol. 9, no. 3, pp. 20-26, March 2009.
[21] R. Plamondon and S. N. Srihari, "On-line and off-line handwriting recognition: a comprehensive survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 1, pp. 63–84, 2000.
[22] M. Kam, K. Gummadidala, and R. Conn, "Signature authentication by forensic document examiners," Journal of Forensic Science, vol. 46, 2001.
[23] G. V. Kiran, R. S. Kunte, and S. Samuel, "On-line signature verification system using probablistic feature modeling", Proceedings of 6th International Symposium on Signal Processing and its Applications, Kuala Lumpur, Malaysia, vol. 1, pp. 355–358, 2001.

P. M. Rubesh Anand received the B.E. degree in Electronics and Communication Engineering from Periyar University, India in 2002, and M.Tech. degree in Advanced Communication Systems from SASTRA University, India in 2004. Since 2005, he is working as a Lecturer in the Faculty of Engineering, Kigali Institute of Science and Technology, Rwanda. Currently, he is pursuing his Ph.D. research at SRM University, Kattankulathur, India. His research interests include communication networks, cryptography and network security.

Gaurav Bajpai received the B.Tech. degree in Computer Science & Engineering from SRMSCET Rohilkhand University, India in 2000, M.Tech. degree in Software Engineering from Motilal Nehru National Institute of Technology, Allahabad, India and Ph.D. degree from Uttar Pradesh Technical University, Lucknow, India in 2006. He was an assistant Professor in the Department of Computer Science and Business Administration, Academy of Medical Sciences and Technology, Khartoum, Sudan from April 2006 to March 2007. Since March 2007, he is working as a Senior Lecturer in the Department of Computer Engineering and Information Technology, Faculty of Engineering, Kigali Institute of Science and Technology, Rwanda. His research interests include software engineering, network routing, network hardware security and bio-medical engineering. He has published more than 30 International Journal and conference papers.

Vidhyacharan Bhaskar received the B.Sc. degree in Mathematics from D.G. Vaishnav College, Chennai, India in 1992, M.E. degree in Electrical & Communication Engineering from the Indian Institute of Science, Bangalore in 1997, and the M.S.E. and Ph.D. degrees in Electrical Engineering from the University of Alabama in Huntsville in 2000 and 2002 respectively. During 2002-2003, he was a post-doc fellow with the Communications research group at the University of Toronto. From Sep. 2003 to Dec. 2006, he was an Associate Professor in the Département Génie des systèmes d'information et de Télécommunication at the Université de Technologie de Troyes, France. Since January 2007, he is a Professor and Associate Dean of the School of Electronics and Communication Engineering at S.R.M. University, Kattankulathur, India. His research interests include wireless communications, signal processing, error control coding and queuing theory. He has published 27 International Journal papers, presented 10 Conference papers in various International Conferences, and co-authored a book on MATLAB. He is also an active reviewer of refereed Journals like the IEEE Transactions on Communications, IEEE Transactions on Wireless Communications, IEEE Communication Letters, IEEE Transactions on Vehicular Technology, International Journal of Network and Computer Applications, International Journal of Computer Communications, and International Journal of Computers and Electrical Engineering.