Handwritten Signatures: An Understanding

Bhushan Thakare
Research Scholar, SGBAU Amravati and Assistant Professor, Sinhgad Academy of Engineering Pune, India

Hemant Deshmukh, PhD
Professor & Head of CSE, Dr.Rajendra Gode Institute Of Tech & Research, Amravati, India

Parikshit Mahalle, PhD
Professor & Head of CE, Smt Kashibai Navale College of Engineering, Pune, India

ABSTRACT
Each user has its own unique signature that is mainly used for purposes such as personal identification and verification of certain documents or legal transactions. But for the same offline signature verification is essential. Currently we have signature verification is inefficient and time-consuming for a large number of documents. To overcome the drawbacks to Signature-based verification, we have seen a growth in online biometric personal verification such as fingerprints, eye scan etc. This paper aims to provide general understanding of signatures, approaches and applications of signature verifications.

Keywords
Signatures, Verification, Forgery

1. INTRODUCTION
Our hand comprises of 27 bones and 40 muscles. Our central nervous system coordinates the contraction, pulling and relaxation of the muscles so to say it also controls the movements of the hand, fingers, wrist etc. The handwritten signatures are the products of such complex systems. They contain certain personal traits and thus are unique among individuals, also, the signatures are hard to imitate or copy. These features led to the use of signature as a biometric [4].

Signature verification has various advantages such as acceptability, a collection that is for storage purposes, and the ability to circumvent [20]. Automatic handwritten signature verification has a wide range of applications, for example, financial institutes can verify bank cheques or credit card transactions automatically; Security systems can use signatures to verify individuals; Organizations can employ automatic signature verification systems to verify certificates and contracts. The construction of such a system has turned out to be a challenging problem.

Personal verification and identification are an actively growing area of research and development. Various biometrics methods are used as well for authentication like face, iris, and fingerprint recognition. Biometric authentication is gaining huge popularity as it is nearly impossible to steal someone's biometric password. It is more safe and secure to use as compared to traditional login password systems [7].

The major factor to promote signatures is e-commerce. For this reason, a lot of biometric applications are being introduced in the area of e-commerce and e-banking systems. Traditional authentication methods e.g. passwords, PIN numbers etc, suffer through major drawbacks. It is easy to guess or recognize one's password also saving the password in the database is not a safe practice as any compromise with the database will reveal thousands of passwords and illegal usage of them. Thus, using biometrics passwords are promoted as they are not easily transferable, are unique of every individual, and cannot be lost, stolen or broken, as they are natural to human beings [8].

The following criteria are used when applying a particular biometric [7].

1. Uniqueness - how unique is the biometric characteristic?

2. Ease of copying and stealing

3. Acceptability by the public; how acceptable is biometric accepted by the public? For example, handwritten signatures are widely accepted as they are used as a proof of authenticity in different fields.

4. Cost to implement the particular biometric data

The human hand in itself gives various characteristics to provide a password such as a palm print, hand geometry, finger geometry and the vein pattern etc. Handwritten signatures are considered a behavioral biometric feature, and it is accepted socially and legally as means of authentication [9].

Handwriting biometrics has a specific relevant component called signature recognition. It extracts writer specific information that makes each signature unique. It can be used in various applications such as PDA, Pocket PC, Tablet PC, or 3G mobile phones that support handwriting capabilities [9].

Handwritten signature verification (HSV) systems are gaining popularity as they are being considered superior to most other biometric authentication techniques mentioned above. They are majorly used in high-security sensitive situations where reliability is crucial as they are expensive and reliable. Signature authentication has been accepted and adapted in the western culture [10]. Although HSV has the potential to gain popularity in the future [11], Miller [12] and Sherman [13] both comment on the fact that this technique will be widely accepted only if it provides more reliability and robustness than the already existing products on the market.

2. HISTORICAL BACKGROUND
Along with the rapid increase of handwriting, the society welcomed Signatures and used it widely for distinctive purposes. Signatures use has been mainly seen with legal and authentication work. As a consequence, people with illicit purposes have attempted to forge signatures as well as handwriting. This has been practiced from early days since the development of writing [4]. The Roman Empire was one of the earliest governments that provided laws for testimony respecting dispute documents by experts. It was later admitted in English-speaking court two centuries ago, in 1792. The practice then became consistent decades later with the passing of the Common Law Procedure Act in England in 1854.

The handwriting was earlier verified manually, which made it dependent on the verifier, his stability, mental and physical conditions etc. Also, the process of verification itself is time-consuming and along comes the high cost. Later with the invention of the computer in the 20th century, researchers started to develop applications for verifying handwriting to overcome these limitations. Automated signature identification/verification is an approach to creating reliable machines to verify or identify signatures and handwriting.

Mauceri [21] reported the first work in on-line signature identification in 1965. This research employed 2350 genuine signatures produced by 45 writers. The accuracy was found to be as high as 90%. In 1966, Kozinets et al. [22] used computers for the off-line authentication system. With the increase in popularity and introduction of PC in 1981, identification using static images became more popular too. In 1986, Ammar *et al.[23]* first proposed a pseudo-dynamic feature extraction technique to extract pressure information from gray images. The reported average error rate (AER) observed was 5%. In 1987, Sabourin and Plamondon [24] reported the first research with the proposed system and testing with 17 professionally almost perfect forgeries. The forgeries were rejected nearly by chance. In 1993, this technique was tested in the well-known case of Daubert vs. Merrell Dow Pharmaceuticals [25].

In spite of the positive results being obtained, the automatic handwritten signature verification using static images is considered less applicable compared to its dynamic counterpart [26]. Thus, it becomes necessary to distinguish between three modes of operation for an automatic signature verification system: offline, online, and hybrid.

3. NATURE OF A HUMAN SIGNATURE

According to the American Heritage Dictionary, a signature can be defined as “the name of a person written with his or her own hand; the act of signing one’s name” [14]. A second definition refers to the whole process of signing which implies the way the signature is made is part of the signature itself. This leads to the hypothesis that the characteristics of the process of signing (i.e. pen pressure, velocity, stroke, etc.) are unique to every individual [15].

The first definition states that a signature is a static two-dimensional image not containing any time-related information and the second definition is based on the dynamic features of the process of signing [15].

Signatures can have many forms such as people use their own names as a signature or maybe initials, or using signatures that are hardly related to their names [10] and, as Brault and Plamondon [16] said, some signatures may be quite complex while others are simple and can be forged easily.

Ruth Rostron [17] explains the graphology of a handwritten signature used to analyze and reveal the personality of an individual. She describes that the variability in the signatures of people may vary in a number of ways, including the individual’s mood at the moment

Gubta [10] points out that if two signatures of the same person were identical, they could be automatically considered as a forgery by tracing. From experts’ point of view, successive signatures of the same person will also differ, both globally and locally and may also differ in scale and orientation. Despite these variations, it is said that these signatures will still have the same characteristics, such as the slant angle and the pressure, classifying them as genuine signatures.

It has also been suggested that human experts are very good in identifying forgeries but perhaps not so in verifying genuine signatures. For instance, in a detailed study, Herbst and Liu [18] cite references, state that signature experts managed to reject or classify as no-opinion as high as 25% genuine signatures while accepting no forgeries. Untrained personnel accepted up to 50% forgeries.

4. MOTIVATION AND NEED HANDWRITTEN SIGNATURES

A signature is a handwritten and often stylish presentation on one’s name or a certain mark that one writes on a document to serve as an identity. The writer of this signature is called a signatory or signer. A signature must not be confused with an autograph. An autograph is an artistic signature that is meant for the public eye to see whereas a signature is always kept private or hidden [40].

The signature is primarily evidential i.e. it gives evidence of [7]:

1. The provenance of the document (identity)
2. The intention (will) of an individual with regard to that document

For example, the role of a signature in many consumer contracts is not solely to provide evidence of the identity of the contracting party, but also to provide evidence of deliberation and informed consent which means that the contracting party was indeed present and has agreed to the terms and conditions if any.

In many countries, signatures are witnessed in the presence of a notary public to sign any legal document or so. On legal documents, an illiterate signatory can make a "mark", and a literate witness signs the same document. In some countries, illiterate people place a thumbprint on legal documents in lieu of a written signature [40].

5. MODES OF OPERATION: ON-LINE, OFFLINE, AND HYBRID

Based on the types of information available, the attainment of a signature verification system varies. It is assumed that a signature verification system would give high accuracies obtained from online systems.

If the input information is represented as a temporal function, the system is considered as an on-line verification system. This stream of information is captured on-the-fly such as when a person writes using a stylus and tablet, digitizer pen, or touch screens. The data obtained may be local pressure, acceleration, speed, the number of strokes, and order of strokes.

Various types of information being available leads to the large performance gap between **online** and other modes of operation. On-line data can be used to generate static signature images. This mode of verification is suitable wherever the result is required as soon as clients’ finish their writing, for example, points of sale or receptions.

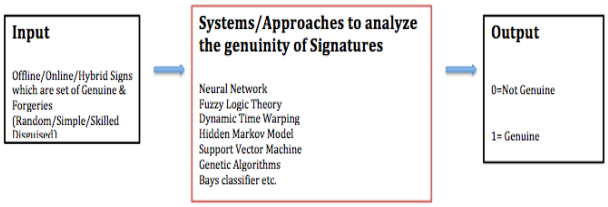
When the process is done using the static signature image solely, the verification process is called **offline**. This does not require any specialized hardware. The drawback is that the amount of information obtained is much more difficult to be interpreted. Also, the dynamic information is difficult to recover. The recovery requires professional skills and techniques. These disadvantages prevent offline systems from yielding better results. The expert document analysts suggest

that the detection of skilled forgeries requires both static and dynamic information.

In the **hybrid mode**, the verification of signature image is performed with reference to the previously registered on-line data. This approach often includes the estimation or recovery of the trajectory from the scanned image before comparing it with the properties of the recovered trajectory. Investigations employing this approach include those conducted by Qiao *et al.* and Zimmer *and* Ling [2].

6. SIGNATURE VERIFICATION TECHNIQUES

For the verifications of signatures, input to the system may be genuine or forgery signs. System will process using some algorithms to find the genuinity the signs. Below is the block diagram of signature verification system and techniques of the same is explained briefly.



Block Diagram of Signatures Verifications

Online and Offline Signature verification systems are categorized in the following two groups.

1. **Offline methods** (also referred to as **static**)
   - No information available at the time of signing the signature.
   - A scanned image of the signature is available.
2. **Online methods** (also referred to as **dynamic**)

Time-related information in the form of the p-dimensional function is available, where p represents the number of features of the signatures, such as the pressure of the pen, velocity etc [8 & 19].

Although online methods have proved to be more accurate as they possess the dynamics of the signature as extra knowledge, offline methods are also essential in the areas where the customer is not present at the time of verification. That is, no knowledge is available describing the process of signing. For instance, verification of signature during payment processing of cheques could only be managed by an offline method as no online characteristics can be extracted.

6.1 Offline Signature Verification Methods

The first approach to solving the signature verification problem was offline signature verification. It discriminates genuine signature from the forged ones using static images. They have only the static image containing the signature as an input, without any knowledge of the signing process. A few difficulties that are faced by the offline systems can be noise on the image, different pen tips and width can produce different shapes [7].

Offline methods were always involved in random and simple forgeries as it is difficult to distinguish genuine from the forged, whereas skilled forgeries are mainly tackled by online methods. Offline signature verification methods for detection of skilled forgeries, is still an open research question [7].

6.2 Online Signature Verification Methods

On-line signature verification is based on the dynamic features of the process of signing. The fact that online verification contains more information, about the process of signing, the accuracy of the recognition is significantly higher than an offline method that does not have any kind of information of the signing process [8].

A special hardware to measure the dynamic characteristics of the signature process is required for online verification methods such as a digitizing tablet, which mainly registers the trajectory and speed of the process together with pressure, pen tip position and other characteristics. The combination of these characteristics are said to be unique to every individual [8].

The dynamic signature verification process is divided into two broad groups: functional and parametric. In the functional case, the decision-making process is constructed on functions in which the input values constitute the feature set which is measured by the equipment. However, in the parametric approach, the parameters of the measured signal are considered as the feature sets [8].

The basic methodology for both methods is almost the same. The methodology involves data acquisition, pre-processing, feature extraction, decision-making, and performance evaluation [10]. Offline methods seem to be more practical than online methods, but more challenging, as only static characteristics are available from the signature image [9].

7. TYPES OF SIGNATURES

There are three main types of signatures: genuine signatures, forgeries, and disguised signatures. Whilst a certain degree of stability is observed in genuine signatures, the forgeries produced by the same forger exhibit significant variations depending on the skill of the forger as well as the amount of information about the genuine signature target that is exposed to the forger. It is widely agreed that the intra-personal variance [27] is smaller than the interpersonal variance. The verification of signatures is possible only if this crucial assumption holds.

7.1 Genuine Signatures

A genuine signature is when an authentic writer produces his own signatures under normal conditions. It isn't restricted by any rules. They are free drawings and may not convey any meaning. In many cases, genuine signatures are unreadable. Although the signatures of an individual may appear very similar, it is widely agreed that signatures are produced differently each time an authentic writer signs. Simply saying, no two signatures are geometrically identical. Hence, when presented with two identical signatures, at least, one of them must be a forgery [4]. Few factors affect the signature of every person such as country, age, time, habits, and psychological or mental state, physical and practical conditions [22].

Genuine signatures can only be produced when the subject is conscious and willing to write in the usual manner. It differs from some other forms of biometric such as fingerprints or DNA as they can still be used for authentication when an individual is unconscious and unaware of its surrounding.

7.2 Forgery

Forged signatures are the handwritings of an impostor with the purpose of it being recognized as genuine signatures of another individual. The dissimilarities between forgeries and genuine signatures originate from the differences between the skilled motor programs responsible for the generation of signatures in the brain of authentic writers and forgers.

As compared to the genuine signatures, the characters of the forgeries are larger. The curves may become angles and vice versa. Strokes may be terminated suddenly when they should be smooth. Redundancy such as strokes or even characters occurs. The quality of lines can be poor; other differences that may occur include punctuation, local or global pressure, baseline, or spacing and what not. Personal writing characteristics of the imitators can even be exposed in their forgeries. Researchers believe that most of these characteristics cannot be modeled and computed for automatic signature verification [28].

The genuine signatures are produced by consistent, skilled, and smooth automated executions of a chain of motor commands in the brain of the authentic signer. Conversely, the visual feedback mechanism in the forger's brain interferes with the signing process and causes inconsistent, unskilled, and hesitance sub-commands. However, the forgers can become more skilled through practice and significant improvements were observed when motivated [29].

As summarized [30] the forgeries belong to one of the following six categories ordered by level of verification difficulty:

1. Forgeries produced without the knowledge of either writer's name or the signature image of the targeted individual: They may significantly differ from genuine signatures in both size and shape and are very easy to recognize. The forgery can even be forger's own genuine signature. In the literature, they are often named *Random Forgery [31]*, *Zero Effort Forgery*, *Simple Forgery [32]*, or *Substitution Forgery [22]*.

2. Forgeries produced with knowledge about the genuine writer's name only: Hanmandlu *et al. [33]* categorized this type of signature as a *Random Forgery* whilst Justino *et al. [31]* categorized this type as a *Simple Forgery*. Occasionally, some researchers may call these *a Casual Forgery [34]*. This type of forgery is supposed to be the most popular although they are not hard to detect.

3. Forgeries produced by inexperienced forgers without the knowledge of their spelling after having observed the genuine specimens closely for some time: are categorized as *Unskilled Forgeries* by Hanmandlu *et al [33]*.

4. Forged signatures produced after examining closely and practicing unrestrictedly with the images of genuine signatures by non-professional forgers are categorized as *Freehand Forgery [27]*, *Simple Forgery/Simulated Simple Forgery [32,35]*, and a *Targeted Forgery* by Huang and Yan [36].

5. *Skilled forgery* refers to the forgeries produced by professional forgers or people possessing knowledge in handwriting analysis or experience in copying signatures [33]. Examining this type of forgery is the most challenging task even for professionals as their appearance resemble genuine signatures and have overall pictorial accuracy. In their signature verification research using forgeries produced by professional forgers, Sabourin and Plamondon [37] reported that the FAR for skilled forgeries was as high as 47%. There is little doubt that the highly skilled forgeries are potentially more stable than genuine signatures. Totty [40] reported the case of an individual whose forgeries exposed no common symptoms of forgery such as tremor, poor line quality, hesitation, or pen lifts.

6. Forgeries produced by tracing a genuine signature: Huber and Headrick [4] called them *Traced forgery*. Forgeries of this type cannot be detected without detailed examination, as their shape, size, and line trajectory is identical to genuine signatures. Consequently, automatic detection of this forgery type requires the questioned signature to be acquired in color at a higher resolution and must be done at line quality level.

Different types of forgeries may require a different verification approach. Whilst the verification accuracy for random forgeries has reached an error rate below 0.1% in the literature, the verification accuracy of targeted and skilled forgeries remains a major problem.

7.3 Disguised Signature

Disguised signatures are the signatures which are produced under the situations where an authentic signer produces the signatures to reject the authenticity of the signed documents later in future [4]. These signatures are produced by authentic users and resemble the genuine signatures, but they contain features which are often found in forgeries. This type of signature has recently been brought to the attention of the automatic signature verification community by the 4NSigComp2010 signature verification competition [39] at the ICFHR '10 international conference.

8. HANDWRITTEN SIGNATURE VERIFICATION (HSV) APPLICATIONS

There are many areas in which HSV technique can be applied, such as the following:

8.1 Financial Transactions

The signature is the most preferred method of authentication due to its convenience. But recent events have shown that it has become easy to forge a handwritten signature which has ultimately increased monetary losses [11]. For example, cheque and credit card frauds, according to A.Kholmatov [7], MasterCard estimates a $450 million loss each year due to credit card fraud.

8.2 Online Banking Transactions

In order to acquire the handwritten signature of the user, a digitizing tablet is used. This saves the users from the pain of remembering the password and PIN codes. Thus, this capturing of static and dynamic features together makes the handwritten signature unique to each and every individual which is also very difficult to forge [11].

8.3 Cheque Processing

The cheque processing flow also consists of a signature verification system, in which the cheques are scanned and are compared with the corresponding legitimate signatures of the legitimate individuals stored in the database. Most of the process is digitized and human intervention will only be required if the signature being processed will result above a specific threshold [11].

8.4 Credit Cards

Credit cards have been in great use, but at the same time highly vulnerable to forgeries. From the existing approaches

to reduce credit card frauds, none of them has been perfect enough to provide 100% full proof. This is due to the lack of competitive advantage or reliability issues as stated by Gubta and McCabe [10].

8.5 Computer User Authentication

HSV systems can also be used to access computer systems like the OS and information system, replacing the traditional password system. The basic requirement would be to connect a digitizing tablet with each workstation to capture signature details [10].

8.6 Passports

HSV systems can be used in passport validation process too. At the time of issuing a passport to a person, he/she is required to visit an authorized an office, where he/she has to provide a sample of signature. This signature is electronically captured on the magnetic strip of the passport. At the point of entry of another country, the customer has to sign on a graphics tablet, which is compared with the reference signature stored on the magnetic strip [10].

9. ISSUES AND CHALLENGES

1. To find the skilled/simulated forgeries.
2. To understand the physical and physiological parameters of the signer.
3. To find random and simple forgeries also.
4. To design the algorithm, this reduces the time complexity.

10. CONCLUSION AND FUTURE SCOPE

In recent years, along with the extraordinary diffusion of the Internet and a growing need for personal verification in many daily applications, automatic signature verification is being considered with renewed interest. Automatic signature verification is a very attractive field of research from both scientific and commercial points of view. In recent years, along with the continuous growth of the Internet and the increasing security requirements for the development of the e-society, the field of automatic signature verification is being considered with renewed interest since it uses a customary personal authentication method that is accepted at both legal and social levels. Thus, in the era of e-society, automatic signature verification should not be restricted to academics and research laboratories only.

11. ACKNOWLEDGMENTS

Our thanks to the experts Dr. Vilas M. Thakare, Dr. Pravin Karde and Prof. Laxmi Thakare.

12. REFERENCES

[1] R. Jayadevan, S. R. Kolhe, P. M. Patil, U. Pal. *Automatic processing of handwritten bank cheque images: a survey.* In *International Journal on Document Analysis and Recognition, SPRINGER,*16 July 2011.

[2] Stephan Armand, Michael Blumenstein, and Vallipuram Muthukkumarasamy. Off-line signature verification based on the modified direction feature. In *Proceedings of the* 18*th International Conference on Pattern Recognition (ICPR '06)*, pages 509–512, Hong Kong, 2006.

[3] Offline Handwritten Signature Verification using Radial Basis Function Neural Networks.

[4] R. A. Huber and A. M. Headrick. *Handwriting Identification: Facts and Fundamentals*. CRC Press, Boca Roton, 1999.

[5] S. Impedovo and G. Pirlo. Verification of handwritten signatures: an overview. In 14*th ICIAP*, pages 191–196, 2007.

[6] R. Plamondon and S. N. Srihari. Online and off-line handwriting recognition: a comprehensive survey. *PAMI, IEEE Trans. on*, 22(1):63–84, 2000.

[7] Anatolyevich Kholmatov Alisher, 'Biometric Identity Verification Using On-Line & Off-Line Signature Verification', MSc Sabanci University, (2003).

[8] Kalenova Diana, 'Personal Authentication Using Signature Recognition', Department of Information Technology, Laboratory of Information Processing, Lappeenranta University of Technology, (2004).

[9] Likforman-Sulem L., Garcia-Salicetti S., Dittmann J., Ortega-Garcia J., Pavesic N., Gluhchev G., Ribaric S. and Sankur B, 'Report on the hand and other modalities stated of the art', Biometrics for Secure Authentication, (2005).

[10] Gubta G. and McCabe A., 'A Review of Dynamic Handwritten Signature Verification', Department of Computer Science, James Cook University Townsville, Qld 4811, Australia, (1997).

[11] Saista Sarl, 'Signature Verification', URL: http://www.timgad.net/html/signature.html [cited 10/01/2006].

[12] Miller B., 'Vital Signs of Identity', IEEE Spectrum, 22-30 (1994).

[13] Sherman R.L., 'Biometric Futures', Computers & Security, 11, 128-133 (1992).

[14] American Heritage Dictionary, 3rd Edition, ver. 3.6a, (SoftKey Intl. Inc., 1994).

[15] Pacut A. and Czajka A., 'Recognition of Human Signatures', Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks, 2, 1560-1564 (2001).

[16] Brault J. and Plamondon R., 'A Complexity Measure of Handwritten Curves: Modeling of Dynamic Signature Forgery', IEEE Transactions on Systems, Man, and Cybernetics, 23(2), 400-413 (1993).

[17] Rostron R., 'The Graphologist', The Journal of the British Institute of Graphologists, 22(2), 28-38 (2004).

[18] Herbst N.M. and Liu C.N., 'Automatic Signature Verification Based on Accelerometry', IBM J Res Dev, 21, 245-253, 1977.

[19] Pacut A. and Czajka A., 'Recognition of Human Signatures', Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks, 2, 1560-1564 (2001).

[20] A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1):4–20, 2004.

[21] A. J. Mauceri. Feasibility study of personnel identification by signature verification. Technical report, Anaheim, CA, 1965.

[22] R. Plamondon and F. J. Maarse. An evaluation of motor models of handwriting. *Systems, Man and Cybernetics, IEEE Transactions on*, 19(5):1060–1072, 1989.

[23] M. Ammar, Y. Yoshida, and T. Fukumura. A new effective approach for off-line verification of signatures by using pressure features. In 8*th Intl. Conf. on Pattern Recognition*, pages 566–569, Paris, 1986.

[24] R. Sabourin and R. Plamondon. On the implementation of some graphometric techniques for automated signature verification systems: a feasibility study. In *Third Intl. Symp. on Handwriting and Comp. App.*, pages 160–162, Montreal, 1987.

[25] Graham Leedham and Vladimir Pervouchine. Validating the use of handwriting as a biometric and its forensic analysis. In Umapada Pal, Swapan K. Parui, and Bidyut B. Chaudhuri, editors, *Document Analysis*, pages 175–192. Allied Publishing Ltd., 2005.

[26] Weiping Hou, Xiufen Ye, and Kejun Wang. A survey of off-line signature verification. In *Intl. Conf. on Intelligent Mechatronics and Automation*, pages 536–541, 2004.

[27] R. Plamondon and G. Lorette. Automatic signature verification and writer identification -the state of the art. *Pattern Recognition*, 22(2):107–131, 1989.

[28] Vamsi K. Madasu. *Automatic Bank Check Processing and Authentication using Signature Verification*. Ph.D. thesis, Queensland University, Brisbane, Australia, 2006.

[29] Christopher J. C. Burges. A tutorial on support vector machines for pattern recognition. *Data Mining and Knowledge Discovery*, 2(2):121–167, 1998.

[30] Vu Nguyen, Michael Blumenstein, Vallipuram Muthukkumarasamy, and Graham Leedham. Off-line signature verification using enhanced modified direction features in conjunction with neural classifiers and support vector machines. In *Proceedings of the* 9*th International Conference on Document Analysis and Recognition (ICDAR '07)*, pages 734–738, Paranã, Brazil, 2007.

[31] Edson J. R. Justino, Flavio Bortolozzi, and Robert Sabourin. A comparison of SVM and HMM classifiers in the off-line signature verification. *Pattern Recognition Letters*, 26(9):1377– 1385, 2005.

[32] M. A. Ismail and Samia Gad. Off-line arabic signature recognition and verification. *Pattern Recognition*, 33(10):1727–1740, 2000.

[33] Madasu Hanmandlu, Mohd Hafizuddin Mohd Yusof, and Vamsi Krishna Madasu. Off-line signature verification and forgery detection using fuzzy modeling. *Pattern Recognition*, 38(3):341–356, 2005.

[34] Weiping Hou, Xiufen Ye, and Kejun Wang. A survey of off-line signature verification. In *Intl. Conf. on Intelligent Mechatronics and Automation*, pages 536–541, 2004.

[35] M. A. Ferrer, J. B. Alonso, and C. M. Travieso. Offline geometric parameters for automatic signature verification using fixed-point arithmetic. *IEEE PAMI, Trans. on*, 27:993–997, 2005.

[36] Kai Huang and Hong Yan. Off-line signature verification using structural feature correspondence. *Pattern Recognition*, 35(11):2467–2477, 2002.

[37] R. Sabourin and R. Plamondon. On the implementation of some graphometric techniques for automated signature verification systems: a feasibility study. In *Third Intl. Symp. on Handwriting and Comp. App.*, pages 160–162, Montreal, 1987.

[38] R. N. Totty. Skilled copies of signatures. Technical report, Chicago, 1995.

[39] Marcus Liwicki, C. Elisa van den Heuvel, Bryan Found, and Muhammad Imran Malik. Forensic signature verification competition 4nsigcomp2010 - detection of simulated and disguised signatures. In *ICFHR*, pages 715–720, 2010.

[40] Signature. URL: https://en.wikipedia.org/wiki/Signatures

13. ABOUT AUTHORS

Bhushan Thakare, Male, is a Assistant Professor at the Sinhgad Academy of Engineering, Pune, India. He is currently working toward the Ph.D. degree in the Computer Engineering, Research Center at Computer Science Engineering Department, Sant Gadge Baba Amravati University, Amravati, India. His research interests include Digital Image Processing, Computer Networks and Data Structures. His teaching interests include Data Structures, Object-Oriented programming, Discrete Structures and Object Oriented Modelling & Design.

Dr. Hemant Deshmukh, Male, is Professor and Head of Computer Science Engineering at Dr. Rajendra Gode Institute of Technology & Research, Amravati, India. He is National Executive Council Member of ISTE New Delhi as well as IETE Amravati Local Centre. He is fellow member of Institution of Engineers (India) and life member of CSI. He has 21 years of experience in teaching & research. He has published more than 156 International & National conference/journal papers.

Dr. Parikshit Mahalle, Male, is IEEE member, ACM member, Life member ISTE and graduated in Computer Engineering from Amravati University, Maharashtra, India in 2000 and received Master in Computer Engineering from Pune University in 2007. From 2000 to 2005, was working as lecturer in Vishwakarma Institute of technology, Pune, India. From Aug 2005 to 2013, he was working as an Assistant Professor and from March 2013, he is working as Professor in Department of Computer Engineering, STES‟s Smt. Kashibai Navale College of Engineering, and Pune, India. He is Ph.D. in wireless communication at received at Center for TeleInFrastruktur (CTIF), Aalborg University, Denmark. He published 25 papers at national and international level. He has authored 5 books on subjects like Data Structures, Theory of Computations and Programming Languages. He is also the recipient of "Best Faculty Award" by STES and Cognizant Technologies Solutions. His research interests are Algorithms, IoT, Identity Management and Security.