DUPLICATE SIGNATURE DETECTION

[1]S. UMA - M.E, [2]P. KARTHIK, [3]M. KAVIN, [4]M. ARUN PANDIYAN

[1]ASSISTANT PROFESSOR, [2,3,4]IV YEAR
DEPARTMENT OF CSE
PAAVAI ENGINEERING COLLEGE (AUTONOMOUS)
NAMAKKAL, TAMILNADU.

***Abstract*- This article will take an in-depth look at the design and implementation of the negative signature technique and explain the important role it plays in data analysis, fraud prevention, and content management. The importance of this process in ensuring that information is accurate and correct is investigated and the necessity of effective and efficient solutions is emphasized.**

INTRODUCTION:

Duplicate signature detection is an important feature in many fields to protect the integrity of information. This section introduces the importance of the system and demonstrates its applications in data analysis, fraud prevention, and content management. The need for a reliable copy signature system has been eliminated.

SYSTEM SPECIFICATION:

The success of the signature execution depends on the hardware and software system specified as a function operation.

HARDWARE REQUIREMENTS:

Processor: Dual-core processor or higher; Might be good for computing needs.

- Dual-core processor or higher is recommended to handle computing tasks.
- This option is designed to provide the processing power required for image analysis, extraction and signature matching.

RAM: At least 4 GB RAM to ensure good performance and memory

- The system must have at least 4 GB of RAM to ensure proper operation and performance.
- Adequate RAM capacity is required to manage complex operations and achieve efficient memory usage when processing images and files.

Storage: At least 50 GB free space to meet system requirements information storage.

- It is recommended to have at least 50 GB of free space to accommodate the system's data storage.
- This is enough storage capacity to match the capacity of the storage system for signature images, rendering files, and other required files.

Device: Used to capture high quality signature images from a signature device such as a pen or touch screen.

- Hardware includes the signing device such as a pen or touch screen.
- This tool is essential to capture good signals and good signatures and provide accurate and reliable input for further processing.

REQUIRED SOFTWARE:

Software Requirements and Functional Description:
The software components of the Duplicate Signature Detection System have been selected to ensure compatibility, versatility and functionality. The following description details each required software and its role in completing major tasks:
Functionality:
Description: This system is designed to work with and is compatible with Windows. Windows and Linux environments to meet different users.
Rationale: Compatibility supports broad audiences by allowing users to seamlessly integrate the duplicate signature detection system into their existing operating environments.
Programming Language: Python:
Description: Python has been chosen as the preferred language due to its versatility and library support.
Why: Python's versatility allows a wide range of functions to be used, while its rich library ecosystem, including image processing libraries and machine learning libraries, enables rapid development and execution of code.
Database: MySQL:
Description: MySQL is used to store, store and manage quality data.

Key Points: MySQL is a reliable and widely used database management system and provides a solid foundation for secure storage and management of databases. document signature. It helps to make the most of data during the matching period.
Framework: OpenCV for Image Processing; TensorFlow for machine learning:
Description: TensorFlow is integrated for machine learning while OpenCV is used for graphics.
Rights: OpenCV offers a wide range of tools for image processing to enable the development of high-quality graphics. TensorFlow is a powerful machine learning framework that can use similar signatures to improve the accuracy of search equations.

REQUIREMENTS:
1. Login:
Description: The system must support security and user-friendly login functionality, No problem .
Principles: Secure access ensures authorized access to the system and protects the integrity of stored signature information.
2.Previous Image:
Description:Use technology to improve image quality and simplify data entry.
Principles: Improving image quality and optimizing input data will help
3. Feature extraction:
Plag: Image processing algorithms that are complex to use to extract relevant features from image signatures.
Key: Feature extraction is an important step in preparing matching data to ensure that the system can identify important features in the signature image.
4. Signature matching:
Description: Uses machine learning algorithms to compare extracted features and identify duplicate signatures.
Principle: Machine learning provides more accurate detection by increasing the body's ability to recognize patterns and similarities.
5. Repository Integration:
Description: Create a secure and reliable warehouse model for storing and managing signature data.
Rationale: Storage increases the efficiency of data recovery during synchronization and helps increase the overall efficiency of the system.
6. User Interface:
Description: A simple and user-friendly interface is designed to allow users to seamlessly access, search and verify the signature file .
Reasons: The user-friendly interface improves the user experience, making it easier for users to interact with the system, access information and interpret positive results.

DATAFLOW DIAGRAMS:
The Level 0 state diagram can be used as a high-level representation of the entire replica signature system. It provides a bird's eye view, captures the interaction of the system with the external environment and addresses the underlying processes.
Level 0 - State Diagram:
Components:
Process:
Duplicate signature detection system: Represented by an all-encompassing program in the System Function.
External Entity:
User: Describes external entities associated with the system. Users provide input and receive output from a central system.
Signing Database: defined as external storage. It acts as a repository for safe keeping of signatures.
Data flow:
From user to system:
The arrow shows the flow of data from the user to the underlying process of the system, representing users' ideas and requests or questions .
System to User:
The text also shows the flow of information from the central system back to the user, representing system output, results, or responses.
System to Database:
Arrows represent the interaction between the central system and the data signature and describe the storage and retrieval operations.

Purpose:
The drawing content is designed to provide a simple, non-descriptive overview of the entire system and to show the key processes and organizations involved.
Refers to the interaction between users, internal processes, and external data and provides the basis for a more comprehensive understanding of the next level of data flow.
Results:
Clarity: This diagram provides a clear image that helps understand the structure and interaction of the body.
Scope Description: Defines the boundaries of the system, focusing on important external areas and their relationships with the central system.
Communication: This diagram is a communication tool that helps participants grasp the meaning of the system without diving deep into the difficult problem identified
level 0 content Diagram understood Important for duplicate signature detection system A starting point is to ground the topic in more detail in the next stage of the data flow diagram. 3.1 Level 0 - Context Graph:
Level 0 context graphs as a high-level representation of the entire duplicate signature system. It provides a bird's eye view, captures the interaction of the system with the external environment and addresses the underlying processes.
Components:
Process:
Duplicate signature detection system: Represented by a program that encompasses everything in the System Function.
External Entity:
User: Describes external entities associated with the system. Users provide input and receive output from a central system.
Signing Database: defined as external storage. It acts as a repository for safe keeping of signatures.
Data flow:
From user to system:
The arrow shows the flow of data from the user to the underlying process of the system, representing users' ideas and requests or questions .
System to User:
The text also shows the flow of information from the central system back to the user, representing system output, results, or responses.
System to Database:
Arrows represent the interaction between the central system and the data signature and describe the storage and retrieval operations.
Purpose:
The drawing content is designed to provide a simple, non-descriptive overview of the entire system and to show the key processes and organizations involved.
Refers to the interaction between users, internal processes, and external data and provides the basis for a more comprehensive understanding of the next level of data flow.
Results:
Clarity: This diagram provides a clear image that helps understand the structure and interaction of the body.
Scope Description:Defines the boundaries of the system, focusing on important external areas and their relationships with the central system.
Communication: This diagram is a communication tool that helps participants understand the meaning of the system without delving into the depths of the identified difficult problem
Level 1 - Overview:
The Level 1 Data Flow Diagram (DFD) provides a detailed description of the main processes in a single signature. This level of hierarchy also divides the entire process into key processes, each of which contributes to the integration and processing of data.
Component:
Process:
1. Signature input: Represents the initial stage of the system that receives signature input from the user or external device .
2. Image pre-processing: It involves improving the quality of the image signature through post-processing before further analysis.
3. Feature extraction: Use image processing algorithms to extract features from image signatures. 4. Signature Matching: There are machine learning algorithms that compare extracted features to correctly identify duplicate names.
5.Database interaction:Explain the process of capturing and storing signature information in a database.
File storage:

File signature: secure storage location of the file signature; Useful for recovery during pairing.
Data flow:
User to signature entry: Arrow indicates the flow of signature data from the user to the signature entry process, starting the duplicate signing Section detection program.
Signature feedback for pre-images: Recommend changes to signature data from input to pre-images before rendering to improve quality.
Image preprocessing for feature extraction: Describes a seamless process from preprocessed signature data to feature extraction.
Feature extraction for signature matching: means the extracted features are passed to the signature process where the algorithm shows the duplicate signature.
Signature comparison for data interaction: Describes the interaction between data through the signature matching process, including data storage and storage.
Usage:
Level 1 DFD provides a detailed description of the main properties, providing a better understanding of how the material is used in the system.
Each subprocess is unique for the general purpose of verifying equal signature by specifying the order of operations.
Advantages:
Procedure Guide: Provides a more detailed understanding of the operation of the system by clearly defining the individual responsibilities and contributions of each process.
Logical Organization: This diagram shows the system process from signature to database interaction by logically organizing the data flow.
Detailed Planning: Level 1 DFD paves the way for a detailed review of each process for a deeper analysis of the job.
Phase 2 - Signature Matching:
The Phase 2 Data Flow Diagram (DFD) provides a complex view of the signature matching process in the signature matching process. This level of detail drills down into the specific steps involved, showing the interaction between the machine learning algorithm and specific data.
Components:
Process:
1.Feature extraction: forms the basis of the signature by expressing the extraction of relevant features from signature images. next comparison subprocess.
2.Signature matching algorithm: Represents the characteristics extracted by the machine learning algorithm responsible for comparing the characteristics.
3.Feature Database: Represents a repository that securely stores features extracted from signature images for use during matching.
Data Storage:
Feature Database: During the feature extraction process, a key database was extracted, which is used as a repository for the relevant features.
Data flow:
Feature extraction to signature matching algorithm: Shows the feature extraction process from the feature extraction sub-process to the signature matching algorithm.
Signature matching algorithm to feature database: Describes the interaction between the signature matching algorithm and the feature database, representing the retrieval of stored features for comparison.
Signature Matching Algorithm for Signature Matching Output: Represents the final output of the signature matching algorithm, which may include a list of duplicates.
Purpose:
Level 2 DFD provides detailed information about the sign comparison process and the interaction between important components.
Shows specific steps on how to use the system to identify the signature equation using machine learning algorithms.
Results:
Algorithm Explanation: This diagram improves the understanding of the machine learning algorithm by describing the object flow and its subsequent interactions with the Database dialog features.
Reference Retrieval: This figure depicting the retrieval of features from the database demonstrates the role of historical data in the matching process. >
Output Visualization: The final output of the signature matching subfunction to the results of the system explains with example.
Use Case Diagram:

A Use Case Diagram is employed to illustrate the interactions between various system components and external entities, outlining specific scenarios or actions. In the context of the duplicate signature detection system, this diagram highlights key use cases such as signature verification and database updates.
Components:
Actors:
User: Represents individuals interacting with the system.
System: Denotes the duplicate signature detection system itself.
Use Cases:
1. Verify Signature: Depicts the user's capability to initiate the verification of a signature using the system.
2. Update Database: Represents the system's functionality to update the signature database.
Associations:
Lines connecting actors and use cases illustrate the relationships and interactions within the system.
Use Case Descriptions:
1. Verify Signature:
Description: Users can utilize the system to verify the authenticity of a signature. This involves submitting a signature for analysis and receiving verification results.
Initiation: Triggered by the user's need to confirm the legitimacy of a signature.
2.Update Database:
Description: The system allows for updates to the signature database. This could involve adding new signatures or modifying existing entries.
Initiation: Initiated by authorized users responsible for maintaining the integrity of the signature database.
Purpose:
The Use Case Diagram provides a concise visualization of the system's functionality, emphasizing the external entities (actors) and their potential interactions with the system.
It focuses on scenarios where users engage with the system to perform specific actions, highlighting the practical applications of the duplicate signature detection system.
Benefits:
User-Centric Perspective: By featuring the user as a primary actor, the diagram emphasizes the system's utility from the end-user's standpoint.
Functional Scenarios: Use cases like signature verification and database updates encapsulate real-world scenarios, showcasing the system's practical applications.
Clarity in Interactions: The diagram provides a clear overview of how external entities (users) can interact with the system to accomplish specific tasks.

Discover the latest technology for signing autographs:
1. Machine Learning Models:
- Signature pattern recognition using supervised learning algorithms including support vector machines (SVM), random forests, and k-nearest neighbors (k-NN).
- Improved the use of unsupervised learning techniques such as clustering and anomaly detection to identify anomalies in signature data.
- Integrating good architecture techniques to improve discrimination of machine learning models.

2. Deep Neural Network (DNN):
- Apply Convolutional Neural Network (CNN) to extract features in signature images.
- Seeking Relational Neural Networks (RNN) to capture progression under negative signatures.

3. Transform Learning:
- Research is transforming the way to improve signature detection performance using advanced learning models on big data.
- Adjust information in related activities, such as data analysis or authoring, to improve the learning ability of the signature model.

4. Integrated method:
- Uses integrated methods, including structural models and support models, to provide predictions from multiple models and correct the whole truth.
- Include diversity in the composite model to increase robustness against multiple signature variations.

COMPARISON OF TRADITIONAL METHODS AND ADVANCED METHODS:
1.Accuracy and accuracy:

- Measure the accuracy and precision of traditional methods such as rule-based and standard models against advanced methods.
- A comparative assessment of the ability to handle changes and the complexity of signature models.

2. Computational Efficiency:

- Check the computational efficiency of advanced algorithms when processing large data sets compared to traditional algorithms.
- Instantly evaluates compliance with situations requiring fast signature verification.

3. Robustness to variability:

- Check the robustness of advanced methods in dealing with signature variability caused by factors such as different writing styles, age and environmental conditions.
- Comparison of changes between traditional signature patterns and dynamic signature patterns. Advanced techniques for evaluating dynamic signature patterns.

4. Generalization across datasets:

- Explore the generalization capabilities of traditional and state-of-the-art methods across different datasets, taking into account changes in sign and context.
- Comparative analysis of changes in the operating characteristics of data.

DISCUSSING THE BENEFITS AND LIMITATIONS OF ADVANCED TECHNOLOGIES:

1. Advantages:

- Improved accuracy: Discuss advanced techniques that are often more accurate due to their ability to capture complex patterns and dependencies.
- Adaptability: Discover how deep learning models adapt to changing signature patterns and demonstrate general capabilities.

2.Limitations:

- Data Dependency: Identify limitations associated with advanced processes that depend on data and may require extensive documentation and may be different for good training.
- Interpretation: Discuss deep interpretation issues in neural networks that can affect the clarity of decision making.

3. Computer Resources:

- Evaluate increasing budget and hardware requirements for training and implementing high-level decision models, including capacity limitations in limited spaces.

4. Ethical considerations:

- Consider the ethical implications associated with the use of advanced technology, including privacy issues and information bias that may affect the integrity of the investigative process.

CHALLENGES OF RESEARCH RECORDING:

1. Contested Attacks:

- Contested Attacks: Contested Attacks on signatures are increasing.
- Strategy: Combines powerful intelligence detection technology with continuous analysis to identify unusual patterns in signatures.

2. Variability of signatures:

- Challenge: The high variability of human signatures makes universal templates difficult.
- Concept: Use machine learning algorithms to adapt and learn from changing signature patterns and improve accuracy over time.

3. Metrics and speed:

- Challenge: Many code signatures need to be completed quickly in a short time.
- Strategy: Use parallel processing and optimization to process large data sets.

4. Dynamic Environment:

- Challenge: Exploration in a dynamic environment with changing context.
- Concept: The combination of context-aware and adaptive models can identify signatures in different situations.

5. Forgery Technology:

- Challenge: Advances in technology are disrupting the signature verification process.
- Strategy: Use analytical methods and develop inference algorithms to identify anomalies that indicate fraud.

Competitive Strategies:

1. Hybrid Methods:

Strategy: Integrate multiple search methods by combining traditional methods with machine learning and artificial intelligence to increase accuracy and usability power.
2. Continuous Learning:
Strategy: Create a model that continuously learns and adapts to new signature patterns, reducing the impact of signature changes and modifications.
3. Blockchain Technology:
Concept: Explore blockchain to securely store and verify signatures, improve integrity and track record signatures.
4.Human-in-the-loop verification:
Strategy: Provide human-in-the-loop verification mechanisms to solve complex and ambiguous problems by leveraging human intelligence and automated systems.

SUGGESTIONS FOR FUTURE RESEARCH:
1. Interpretable Artificial Intelligence in Sign Analysis:
Introduction: Study of interpretable communication technologies to improve the clarity and interpretation of the sign name display model.
2. Biometric Fusion:
Guidance: Explore the fusion of various biometric variables (e.g. fingerprints, facial recognition) with signature recognition to help increase recognition and increase reliability.
3. Standardization and Comparison:
Guidance: Establish standards and benchmarks to facilitate fair comparison and comparison of signature systems.
4. Cross-domain application:
Direction: Examine the adaptability of the duplicate signature detection method in different domains (such as finance, healthcare, and law).
5. Privacy Protection Technology:
Introduction: Privacy protection research to secure sensitive signature information during search.
Strategic review of challenges, planning strategies, and future research directions provides a means to advance the field of signature research. Researchers can focus on these areas to improve the accuracy, efficiency, and usability of signing certificates.

SCIENTIFIC RESEARCH: REAL LIFE RE-RECORDING RESEARCH
1. Financial Institution:
Scenario: A large financial institution that manages many businesses.
Important: Verifying the signature balance is important to prevent fraud such as fake checks or illegal transactions.
Usage: Integration of the best signature analysis to identify and flag suspicious transactions.
Success: Significant reduction in financial fraud, increased customer trust and operational security.
Lessons Learned: Outline immediate and ongoing trends to accommodate fraudulent transactions.
2. Legal documents:
Scenario: Law firms and legal entities have contracts and legal documents.
Importance: Ensuring the accuracy of signed legal documents and preventing fraudulent contracts and agreements.
Usage: Hybrid study combining legal analysis and machine learning models.
Success: Increased accuracy in verifying signatures, reducing disputes and financial losses.
Lessons Learned: Highlights the importance of various methods that combine human intelligence with automated systems for effective results.
3. Medical Information:
Scenario: A hospital manages patient information and medications.
Important: Check the doctor's signature on the prescription to avoid incorrect and unauthorized medications.
Usage: Use signature verification algorithms integrated into the electronic health record (EHR).
Achievements: Improve patient safety by reducing medication administration errors.
Lessons Learned: Recognize the need for integration with existing therapies to ensure high adoption and usability.
4. E-commerce Platform:
Scenario: Online stores handle many digital businesses.
Meaning: Check and prevent unauthorized purchases and delete the account.
Task: Build a machine learning model for real-time analysis of digital signatures related to online businesses.
Success: Reduce fraud thus increasing customer trust and security.
Lessons Learned: Recognize the importance of reform in changing online fraud patterns and continuing to update detection patterns.
5. Government Authentication:

Scenario: Government agencies verify personal information and legal information.
Important: Legalization of signatures on passports, permits and official documents.
Usage: Use advanced signature verification tools for fast, reliable authentication.
Achievements: Improve government processes, increase efficiency and reduce personal fraud.
Lessons Learned: Demonstrates the need for solutions that can handle many authentication requests.

EVALUATION AND RESULTS OF SIGNATURE VERIFICATION:

1. Performance measure:
Accuracy: Measure the overall accuracy of the equation check.
Accuracy: Tests the ratio of the correctly checked equation sign to the checked integer equation. For: Tests whether the fraction of the equal sign is correctly identified by the system.
F1 Score: Measure accuracy and return to provide performance measurement.
2. Test site:
Dataset: Description of the data used, including various diversity, complexity, and content signatures.
Comparison: Check available comparisons for comparison.
Training and testing: Guidelines for classifying data according to training and testing procedures to ensure good evaluation models.
3. Comparison with existing methods:
Basic method: Shows the results of using a traditional signing certificate, such as a rule against rules and standards.
Comparison Metrics: Comparison of accuracy, precision, recall and F1 score between state-of-the-art and baseline.
Highlights: Measurements to determine the importance of performance variables.
4. Verification of the plan:
Verification of the algorithm: presents results using the proposed duplicate signature analysis method.
Robustness testing: Evaluates the robustness of different datasets and changes in signature patterns in different datasets.
Real-time events: Use a research-based and practical approach to protect against known signature events.
5. Computational Efficiency:
Processing Time: Estimate the time required to sign a signature using the proposed method.
Product Usage: Test the performance of the included product.
6. Visual Perspective:
Confusion Matrix: Visual representation of positive, negative, negative and negative.
ROC Curve: The chart represents the balance between the right price and the wrong price.
7. Cross-domain generalization:
Cross-domain performance: Analyze the impact of the proposed method on generalization to different domain datasets.
Training Methodology: Evaluates the impact of learning transitions on model performance across different data sets.
8. Negotiating Conflicts and Conflicts:
Description: Identify and discuss difficult situations.
Mitigation Strategies: Security vulnerabilities in the signature detection process and recommendations for dealing with vulnerabilities.
9. Decision fairness:
Fairness Analysis: Analyze datasets for biases and their impact on algorithmic decision making.
Fairness Measures: Discuss the measures taken to ensure fairness and fairness when signing, especially in sensitive applications.

CONCLUSION

A comprehensive evaluation of the signature equation system provides important insights that are important for progress. The analysis shows that advanced techniques, especially machine learning models and deep neural networks, perform best for detecting signature similarity in different information. The impact on the broader cybersecurity landscape is significant, as strong signature verification tools play a key role in mitigating the risks associated with fraud, unauthorized copying and personal threats. The impact can be extended to many areas such as finance, law, healthcare, and e-commerce, where discovering the reliability of signatures is important. This study highlights the importance of integrating advanced technologies into existing security systems to improve threat protection. As we look ahead, calls to action for further research and development are important. Although advanced methods have shown promising results, continued efforts are needed to address issues related to interpretation, computational efficiency, and ethical considerations. Future research should focus on improving algorithms to maintain good signature models, ensure fairness in the decision-making process, and create benchmarks for comparison. Collaboration between academia, industry and regulatory bodies is essential to develop best practices, promote the use of advanced technologies and sign

environmental practices. By encouraging a commitment to continuous research and development, we can strengthen cybersecurity measures and increase the reliability of signature certificates in the evolving digital environment.

REFERENCES:

1)"Handwritten Signature Verification using Deep Learning" by Eman Alajrami1 , Belal A. M. Ashqar , Bassem S. Abu-Nasser , Ahmed J. Khalil , Musleh M. Musleh , Alaa M. Barhoom , Samy S. Abu-Naser.

2) Online Handwritten Signature Verification System using Gaussian Mixture Model and Longest Common Sub-Sequences

3) Dropout: a simple way to prevent neural networks from overfitting, by Hinton, G.E., Krizhevsky, A., Srivastava, N., Sutskever, I., & Salakhutdinov, R.

4) H. Baltzakis and N. Papamarkos. A new signature verification technique based on a two-stage neural network classifier. Engineering applications of Artificial intelligence, 14(1):95–103, February 2001.

5) R.K. Bharathi and B.H. Shekar. Off-line signature verification based on chain code histogram and Support Vector Machine. In 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pages 2063–2068, August 2013.

6) Peter Shaohua Deng, Hong-Yuan Mark Liao, Chin Wen Ho, and HsiaoRong Tyan. Wavelet-Based Off-Line Handwritten Signature Verification. Computer Vision and Image Understanding, 76(3), December 1999

7) G.S. Eskander, R. Sabourin, and E. Granger. Hybrid writer-independentwriter-dependent offline signature verification system. IET Biometrics, 2(4):169–181, December 2013.

8) Understanding of a convolutional neural network by IEEE

9) Getting Started with Image Preprocessing in Python by Adhinga Fred

10)Peter Shaohua Deng, Hong-Yuan Mark Liao, Chin Wen Ho, and HsiaoRong Tyan. Wavelet-Based Off-Line Handwritten Signature Verification. Computer Vision and Image Understanding, 76(3), December 1999.

11) M. Diaz, M. A. Ferrer, G. S. Eskander, and R. Sabourin. Generation of Duplicated Off-Line Signature Images for Verification Systems. IEEE Transactions on Pattern Analysis and Machine Intelligence, 39(5):951– 964, May 2017.

12) Giovanni Dimauro, Sebastiano Impedovo, Giuseppe Pirlo, and A. Salzo. A multi-expert signature verification system for bankcheck processing. Int. Journal of Pattern Recogn., 11(05):827–844, 1997.

13) S. Djeziri, F. Nouboud, and R. Plamondon. Extraction of signatures from check background based on a filiformity criterion. IEEE Transactions on Image Processing, 7(10):1425–1438, October 1998.

14) J.-P. Drouhard, Robert Sabourin, and Mario Godbout. A neural network approach to off-line signature verification using directional PDF. Pattern Recognition, 29(3):415–424, 1996.

15) A. El-Yacoubi, E. J. R. Justino, R. Sabourin, and F. Bortolozzi. Offline signature verification using HMMs and cross-validation. In Neural Networks for Signal Processing X, 2000. Proceedings of the 2000 IEEE Signal Processing Society Workshop, volume 2. IEEE, 2000.

16) G.S. Eskander, R. Sabourin, and E. Granger. Hybrid writer-independentwriter-dependent offline signature verification system. IET Biometrics, 2(4):169–181, December 2013.

17) M. A. Ferrer, J. B. Alonso, and C. M. Travieso. Offline geometric parameters for automatic signature verification using fixed-point arithmetic. IEEE Transactions on Pattern Analysis and Machine Intelligence, 27(6):993–997, June 2005.

18) M. A. Ferrer, M. Diaz-Cabrera, and A. Morales. Static Signature Synthesis: A Neuromotor Inspired Approach for Biometrics. IEEE Transactions on Pattern Analysis and Machine Intelligence, 37(3):667– 680, March 2015.

19) M.A. Ferrer, M. Diaz-Cabrera, and A. Morales. Synthetic off-line signature image generation. In 2013 International Conference on Biometrics (ICB), pages 1–7, June 2013.

20) Julian Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez, and Javier Ortega-Garcia. An off-line signature verification system based on fusion of local and global information. In Biometric Authentication, pages 295–306. Springer, 2004.

21) C. Freitas, M. Morita, L. Oliveira, E. Justino, A. Yacoubi, E. Lethelier, F. Bortolozzi, and R. Sabourin. Bases de dados de cheques bancarios brasileiros. In XXVI Conferencia Latinoamericana de Informatica, 2000.

22) S. Ghandali and M.E. Moghaddam. A Method for Off-line Persian Signature Identification and Verification Using DWT and Image Fusion. In IEEE International Symposium on Signal Processing and Information Technology, ISSPIT, pages 315–319, December 2008.

23) Almudena Gilperez, Fernando Alonso-Fernandez, Susana Pecharroman, Julian Fierrez, and Javier Ortega-Garcia. Off-line signature verification using contour features. In 11th International Conference on Frontiers in Handwriting Recognition, 2008.

24) Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative Adversarial Nets. In Advances in Neural Information Processing Systems 27, pages 2672–2680. 2014.

25) Yasmine Guerbai, Youcef Chibani, and Bilal Hadjadji. The effective use of the one-class SVM classifier for handwritten signature verification based on writer-independent parameters. Pattern Recognition, 48(1):103–113, January2015.