Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 6, December 2026, pp. 5056~5067
ISSN: 2302-9285, DOI: 10.11591/eei.v15i6.14147

Descriptor-dependent Josephus encryption for cross-script offline signature verification

Ismail Hadjadj[1,2], Abdeljalil Gattal[2], Mouloud Ayad[3]
[1]Laboratoire d'Informatique et de Mathématique, Faculty of Exact Sciences, University of Bouira, Bouira, Algeria
[2]Laboratoire de Vision et d'Intelligence Artificielle, Echahid Cheikh Larbi Tebessi University, Tébessa, Algeria
[3]Department of Electronics, LIS Laboratory, Faculty of Technology, Sétif 1 University, Setif, Algeria

Article Info

Article history:

Received Aug 2, 2026
Revised Sep 11, 2026
Accepted Oct 4, 2026

Keywords:

Cross-script evaluation
Josephus encryption
Local ternary patterns
Offline signature verification
Oriented basic image features
Run-length distributions
Texture descriptors

ABSTRACT

Josephus encryption deterministically rearranges image pixels, but its value for offline signature verification depends on how a descriptor responds to altered spatial neighborhoods. This study evaluates that dependency across scripts under three representation conditions: clear, encrypted, and combined. Four handcrafted representations (local ternary pattern (LTP), oriented basic image features (oBIFs), run-length distribution (RLD), and an LTP–oBIFs fusion) are compared within a writer-independent radial basis function (RBF) support vector machine (SVM) framework. Experiments cover GPDS300, the Dutch and Chinese subsets of SigComp 2011, and the Bengali and Italian subsets of SigWIcomp 2015. Training uses genuine-genuine and genuine-forgery dissimilarity vectors, while testing compares questioned signatures with the mean reference template. The effect of encryption is descriptor- and dataset-dependent. Combined LTP+oBIFs reached 85.06% ACC on GPDS300; clear oBIFs reached 98.08% on Dutch; and clear LTP+oBIFs reached 88.58% on Chinese. For SigWIcomp 2015, the best minimum log-likelihood-ratio costs were 0.0346 for Bengali with combined RLD and 0.0227 for Italian with combined LTP+oBIFs. Josephus encryption can provide complementary evidence in selected settings, but it can substantially degrade orientation-sensitive descriptors, so representation choice should be validated for the target dataset.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Ismail Hadjadj
Laboratoire d'Informatique et de Mathématique, Faculty of Exact Sciences, University of Bouira
10000 Bouira, Algeria
Email: i.hedjadj@univ-bouira.dz

1. INTRODUCTION

In offline verification, a static image of a questioned signature must be classified as authentic or forged. Unlike online systems, offline verification has no direct access to pen trajectory, pressure, timing, or velocity; the decision must be inferred from the appearance of a scanned or photographed trace. This makes skilled forgery detection difficult because genuine samples vary naturally while imitations may reproduce large-scale shape. The problem has consequently remained active across classical pattern recognition, forensic document analysis, and biometric authentication [1]–[5]. Cross-script reliability is particularly relevant to multilingual financial services, e-government authentication, and academic credential verification, where one backend may encounter signatures formed under different writing conventions.

Writer-independent systems learn a common decision rule from multiple writers and can be deployed for identities not used to train the classifier [6]. Their effectiveness depends strongly on the representation used to compare signatures. Early systems relied on geometric, directional, and texture measurements [7]–[12].

Deep convolutional, metric-learning, graph, transformer, hybrid, augmentation, and spatial-transformer approaches later broadened representation learning [13]–[21]. A Siamese formulation with synthetic data also demonstrated cross-dataset transfer under a random-forgery setting [22], while recent reviews summarize the continuing trade-offs between handcrafted and learned representations [23]. Handcrafted descriptors remain relevant when sample counts are limited, computational resources are modest, or an interpretable feature construction is preferred.

Cross-script evaluation introduces an additional difficulty. Signature appearance is influenced by writing habits, stroke density, orientation distribution, and the visual conventions of the underlying script. A representation that is effective for Latin-script signatures may respond differently to Chinese or Bengali signatures. Prior multilingual studies and international competitions have demonstrated that performance can vary substantially across datasets even under a common verification framework [24]–[27]. A controlled descriptor-level analysis is therefore useful before claiming script-independent behavior.

This work studies Josephus encryption, defined here as a deterministic pixel-position rearrangement used to generate an alternative signature representation. The underlying Josephus traversal is a classical cyclic-elimination problem [28]. In image-security literature, Josephus traversals have been combined with diffusion or chaotic maps as components of encryption systems [29], [30]. The present study is deliberately different: it does not claim cryptographic security and does not evaluate key space, entropy, differential attacks, or resistance to cryptanalysis. Instead, the fixed rearrangement is treated as a representation transform that preserves pixel values while replacing their spatial neighborhoods. This distinction separates the present descriptor study from image-encryption studies whose primary objective is confidentiality.

A remaining gap is the lack of a controlled cross-script study that isolates how the same Josephus rearrangement affects different descriptor families. This descriptor-dependent cross-script analysis is the central innovation of the present work.

The research question is: how does Josephus-based pixel rearrangement affect the discriminative performance of different handcrafted texture descriptors across signature datasets and writing scripts? The working hypothesis is that the effect is descriptor-dependent rather than uniformly positive. Three contributions are made. First, local ternary pattern (LTP), oriented basic image features (oBIFs), and run-length distribution (RLD) are examined separately under clear, encrypted, and combined conditions. Second, the experiments are then repeated on five benchmark subsets: GPDS300; Dutch and Chinese SigComp 2011; and Bengali and Italian SigWIcomp 2015. Third, a controlled ablation keeps the pair-generation rule, template construction, normalization, and support vector machine (SVM) configuration fixed so that changes can be attributed primarily to the representation condition. The practical implication is not that encryption should always be added, but that descriptor design should explicitly consider which spatial statistics are preserved or destroyed by a transformation.

The rest of the paper is structured as follows. Section 2 reviews related research. Section 3 defines the Josephus rearrangement and discusses its expected interaction with the descriptors. Section 4 specifies the datasets, representations, classifier configuration, and evaluation protocol. Section 5 presents and interprets the empirical findings, while section 6 summarizes the conclusions and future directions.

2. RELATED WORK

Handcrafted offline signature verification methods typically convert the image into a compact vector and then measure similarity or train a classifier. One-class SVMs with curvelet features were used to model genuine signatures under writer-independent settings [8]. For writer-dependent verification, Serdouk *et al.* [9] integrated gradient-LBP and longest-run cues within an artificial immune recognition framework. Poset-oriented grids represented local structural arrangements [10], while RLDs captured directional continuity using a small number of genuine samples [11]. LTP and oBIFs were previously combined for competition datasets, showing that complementary local texture and orientation cues can support writer-independent verification [12].

Learned representations address the feature-design problem directly. Deep multitask metric learning jointly optimized feature extraction and signature distance [13]. SigNet established a widely used convolutional representation [14], and deep metric learning produced compact signature embeddings [15]. Knowledge transfer from handwriting to signatures was explored with CNN-based contrastive learning [16]. Graph neural networks modeled relations among signature samples [17], while TransOSV used transformer components for holistic and part-based encoding [18]. Hybrid CNN-HOG systems [19], generative augmentation for small real-sample sets [20], spatial-transformer alignment [21], and Siamese learning with synthetic signatures [22] illustrate the diversity of modern learned approaches.

Cross-script and competition studies are particularly relevant to the present analysis. Verifier fusion with random forests was evaluated across languages [24], and multi-script versus single-script training was investigated for offline verification [25]. SigComp 2011 supplied Dutch and Chinese skilled-forgery tasks [26], whereas SigWIcomp 2015 included Bengali and Italian evaluation settings [27]. These benchmarks make it

possible to observe whether a representation behaves consistently across different signature styles without assuming that language content itself is recognized.

The closest prior streams are descriptor fusion and multilingual verification [12], [24], [25] and Josephus-based image transformations [29], [30]. However, these streams do not isolate how one fixed Josephus rearrangement changes different descriptor families under a common cross-script signature-verification protocol.

The present work does not attempt to replace learned representations or establish a universal ranking against systems that use different partitions, forgery types, metrics, and training objectives. Its purpose is narrower: to determine how one fixed Josephus rearrangement changes the response of three interpretable descriptors under a common writer-independent pipeline. This descriptor-dependent perspective distinguishes the study from systems that report only the final performance of a fused clear and encrypted vector.

3. JOSEPHUS ENCRYPTION AND DESCRIPTOR RESPONSE

Let an image contain $L = M \times N$ pixels. Row-major flattening produces the vector $v = [v(1), \ldots, v(L)]$. A Josephus traversal maintains an ordered list A of one-based indices. Starting at position s, every k-th remaining position is selected cyclically, appended to the permutation q, and removed. Counting then continues from the removal position in the shortened list. The encrypted vector is constructed as (1):

$$v_E(i) = v\big(q(i)\big), \qquad i = 1, \cdots, L \tag{1}$$

Here, M and N denote the two spatial dimensions of the image, and their product $L = M \times N$ gives the total pixel count, $q(i)$ is the input index selected for output position i, and $v_E(i)$ is the encrypted-vector value at that output position. From (1) makes the permutation direction explicit: the pixel value at input position $q(i)$ is copied to encrypted position i. Pixel values are unchanged, but their positions and local neighborhoods are rearranged. The permutation is applied before descriptor extraction rather than to descriptor coefficients; each descriptor is therefore recomputed on the rearranged image. Any change in intra-writer consistency or genuine-forgery separation arises indirectly from the descriptor's response to these new spatial neighborhoods.

All experiments use s=100 and k=100, applied once to the complete pixel vector. These values are fixed global design constants rather than dataset-specific optimum parameters. They are intentionally not tuned per descriptor or dataset, because parameter optimization would confound the study's main objective of isolating descriptor response to one common deterministic rearrangement. Consequently, the reported results characterize this fixed Josephus configuration and should not be interpreted as a sensitivity study over s and k. The small example in Figure 1 uses s=1 and k=3 only to make the indexing visible. Algorithm 1 gives the complete indexing procedure in standardized monospaced pseudocode.

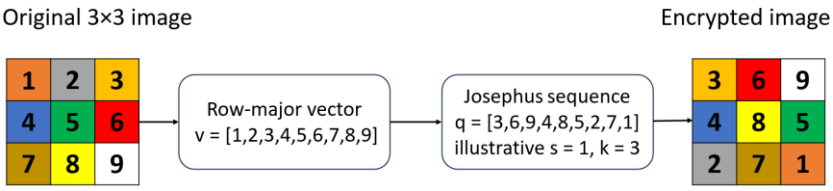


Figure 1. Josephus pixel rearrangement preserving pixel values, illustrated using a 3×3 example (s=1, k=3); all experiments use s=100 and k=100

Algorithm 1. Josephus encryption of a signature image

```
Input: image I of size M × N; parameters s = 100, k = 100
Flatten I row by row into v of length L = M × N
A ← [1, 2, ..., L]; p ← s; q ← empty list
while A is not empty do
    p ← mod(p + k - 2, length(A)) + 1
    append A[p] to q
    remove A[p] from A
    continue counting from the removal position
end while
for i = 1, ..., L do
    vE[i] ← v[q[i]]
end for
reshape vE to M × N and return the Encrypted image
```

3.1. Expected descriptor response

LTP characterizes each local neighborhood by comparing neighboring intensities with the center pixel through a three-level thresholding rule [31], [32]. Josephus encryption replaces the original neighborhood system, so the resulting histogram describes redistributed local contrasts rather than stroke-local texture. This may create complementary evidence when clear and encrypted vectors are concatenated, but the benefit is not guaranteed.

oBIFs assigns local symmetry and orientation classes from derivative-of-Gaussian responses [33], [34]. Because these classes depend directly on coherent edge and ridge direction, pixel rearrangement is expected to damage the structures that make clear oBIFs discriminative. RLD measures consecutive foreground pixels in four directions [11]. Encryption fragments many original runs, yet the new distribution may still encode ink density and fragmentation patterns. Section 5 tests these expectations rather than assuming a uniform gain. LTP, oBIFs, and RLD were selected because they represent complementary local-contrast, orientation/symmetry, and directional-run mechanisms already used in offline signature verification; their different spatial dependencies make the effect of Josephus rearrangement directly testable. HOG, SIFT, and learned CNN features are outside this controlled ablation and are retained as comparison or future baselines rather than mixed into the present descriptor-level experiment.

4. METHOD

4.1. Datasets and evaluation partitions

Five retained subsets cover Latin, Chinese, and Bengali scripts. GPDS300 is derived from the GPDS-960 corpus [35]. The Dutch and Chinese subsets follow SigComp 2011 [26], and the Bengali and Italian subsets follow SigWIcomp 2015 [27]. No CEDAR or SASIGCOM data are included. Table 1 summarizes writer counts, genuine/forged samples, partitions, and metrics. All retained samples are used; the generated genuine–genuine and genuine–forgery training pairs are not artificially balanced by undersampling, oversampling, or class-specific weighting.

Table 1. Retained datasets and evaluation protocols

Dataset/script	Writers and samples	Partition	Reference/questioned protocol	Metrics
GPDS300 Latin/English	300 writers; per writer: 24 genuine and 30 skilled forgeries	Writers 1--150 train; 151--300 test	12 genuine references; 12 genuine and 30 forged questions	ACC, FAR, FRR, AER
SigComp 2011 Dutch Latin/Dutch	54 writers; per writer: 24 genuine and about 12 forged signatures	Organizer-defined competition split	Mean of all official references; official questioned set	ACC, FAR, FRR, AER
SigComp 2011 Chinese	10 writers; per writer: 24 genuine and about 34 forged signatures	Organizer-defined competition split	Mean of all official references; official questioned set	ACC, FAR, FRR, AER
SigWIcomp 2015 Bengali	10 writers; per writer: 24 genuine and 30 forged signatures	Organizer-defined competition split	Mean of all official references; official questioned set	$\hat{C}_{llr}$, $\hat{C}_{llr}^{min}$
SigWIcomp 2015 Italian Latin/Italian	50 writers; per writer: 5 reference and 10 questioned signatures	Organizer-defined competition split	Mean of all official references; official questioned set	$\hat{C}_{llr}$, $\hat{C}_{llr}^{min}$

4.2. Representation pipeline

Each descriptor is evaluated in three conditions. Clear uses the descriptor extracted from the supplied image. Encrypted uses the same descriptor after Josephus encryption. Combined concatenates the two vectors directly. For LTP+oBIFs, the order is [LTP_{Clear}, $oBIFs_{Clear}$, $LTP_{Encrypted}$, $oBIFs_{Encrypted}$]. The rest of the pipeline is identical across conditions, as shown in Figure 2.

4.3. Image handling and descriptors

Images are used in their original supplied form and dimensions. No global grayscale conversion, denoising, cropping, resizing, or image normalization is performed. RLD alone applies descriptor-specific fixed-threshold binarization with MATLAB im2bw(image,0.8). The threshold 0.8 is fixed for all datasets and is not tuned per writer, dataset, or representation condition. Descriptor outputs are used as returned by their extractors; no separate descriptor-level normalization is introduced.

As illustrated in Figure 2, three feature representations are evaluated: clear, encrypted, and combined. The clear representation extracts features directly from the original signature, bypassing Josephus rearrangement, whereas the encrypted representation uses features extracted from the Josephus-rearranged signature. The combined representation concatenates clear and encrypted features. All three representations undergo the same dissimilarity-vector construction and unit-sum normalization stages, followed by independently trained radial basis function support vector machine (RBF-SVM) classifiers for genuine/forged signature verification.

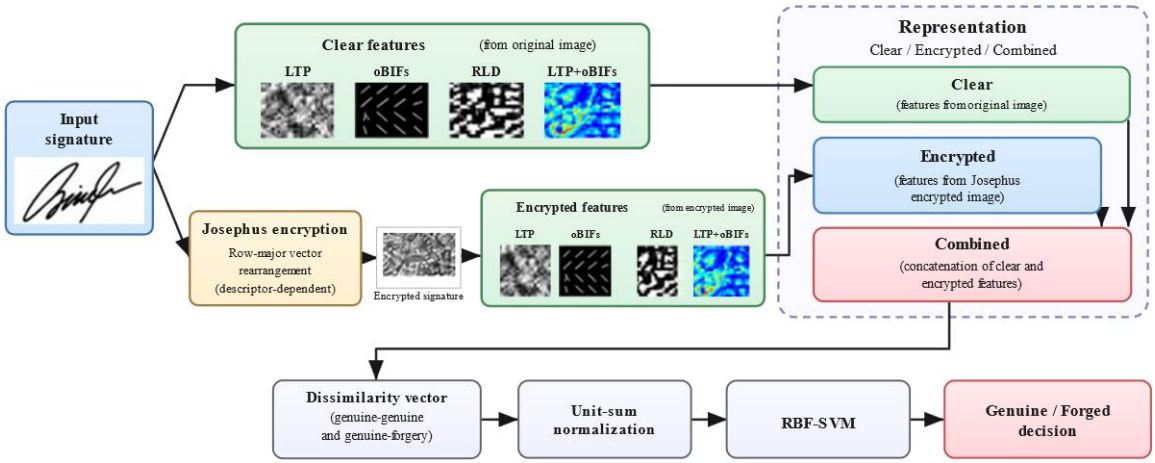


Figure 2. Evaluation pipeline for clear, encrypted, and combined feature representations

Table 2 lists the implementation settings and feature dimensions. For oBIFs, n=4 quantizes local orientation and gives 5n+3=23 histogram classes. The parameter ε controls the flat-class threshold and σ sets the derivative-of-Gaussian scale. Candidate values ε∈{1, 0.1, 0.01, 0.001} and σ∈{2, 4, 8, 12, 16} were evaluated, and the retained pairs were (0.1,4) for GPDS300 and (0.1,16) for all SigComp 2011 and SigWIcomp 2015 subsets. The LTP setting P=1, R=16, and t=0.3 is common to all datasets [31], [32]. RLD retains 100 run-length positions for each of four directions [11].

Table 2. Fixed implementation settings and feature dimensions

Component	Setting	Dimension/model
Josephus encryption	s=100, k=100; one-based indexing; row-major; complete M×N vector; original dimensions retained	--
LTP	P=1, R=16, and t=0.3; upper and lower histograms	4 clear/encrypted; 8 combined
oBIFs	n=4; 23 histogram classes; dataset-specific (ε,σ)	23 clear/encrypted; 46 combined
RLD	im2bw threshold 0.8; horizontal, vertical, left- and right-diagonal; first 100 positions per direction	400 clear/encrypted; 800 combined
LTP+oBIFs	Direct descriptor concatenation	27 clear/encrypted; 54 combined
Dissimilarity	Elementwise absolute difference; nonzero vector divided by its element sum	Same as representation
SVM	fitcsvm; RBF; KernelScale=auto; C=1; Standardize=true; ClassNames=[0, 1]	Separate model per dataset, descriptor, condition

4.4. Dissimilarity generation and classification

Training vectors are generated within each writer. Positive examples contain every unordered pair of genuine signatures. Negative examples compare every skilled forgery with every genuine signature of the same claimed writer. The representation of a pair is the elementwise absolute difference. All generated examples are retained with equal default weight; no class balancing, undersampling, oversampling, or custom cost matrix is used.

During testing, the feature vectors of all reference signatures for an identity are averaged with equal weights. Each questioned signature is compared with this mean reference template through the same elementwise absolute difference. For every GPDS300 test writer, genuine samples 1–12 form the reference set. Genuine samples 13–24 serve as genuine probes, while all 30 skilled forgeries are used as forged probes. Competition subsets use their official reference and questioned folders.

Each nonzero dissimilarity vector x is normalized before classification as (2):

$$x \leftarrow \frac{x}{\Sigma_i x_i} \tag{2}$$

In (2), x_i is the i-th nonnegative component of the absolute-difference vector; zero vectors are left unchanged to avoid division by zero.

A binary SVM is fitted with MATLAB R2017b fitcsvm [36]. The kernel is RBF, KernelScale is automatic, BoxConstraint is 1, predictor standardization is enabled, and ClassNames=[0, 1], where 1 denotes

genuine and 0 forged. For each dataset-descriptor pair, clear, encrypted, and combined are evaluated independently, requiring a separately fitted model for each representation while preserving the same hyperparameters. This design yields 60 fitted models across five datasets, four descriptor families, and three representation conditions. A single execution was performed on a CPU-only workstation running 64-bit Windows 10, equipped with an Intel Core i5-4440 processor (3.10 GHz) and 8 GB of DDR3 memory.

4.5. Evaluation measures

Hard SVM decisions are used for FAR and FRR. FAR measures the fraction of forged queries that the classifier incorrectly accepts as genuine, and FRR measures the fraction of genuine queries that are incorrectly rejected as forgeries. For GPDS300 and SigComp 2011, AER and ACC are computed consistently as (3) and (4):

$$AER = \frac{FAR+FRR}{2} \tag{3}$$

$$ACC = 100 - AER \tag{4}$$

Thus FAR and FRR are error percentages, AER is their equal-weight mean, and ACC is the complementary percentage. For SigWIcomp 2015, the second predict-score column, corresponding to the genuine class, is separated into target and non-target vectors. The raw scores are supplied to the *Cllr* toolkit [37], [38] to compute $\hat{C}_{llr}$ and to the min_cllr routine to compute $\hat{C}_{llr}^{min}$. These values are reported to four decimal places.

4.6. Computational complexity and storage

The computational behavior depends on whether the Josephus permutation is generated for each image or reused for a repeated image size. Algorithm 1 uses dynamic deletion from the ordered index list A. With a conventional contiguous array, each deletion can require compaction of the remaining entries, giving worst-case permutation-generation time quadratic in L and linear auxiliary index storage. Once a permutation q has been generated, applying (1) is linear in L. Therefore, for repeated signatures of identical dimensions, precomputing and reusing q removes the quadratic generation step from subsequent images; for heterogeneous image dimensions, a permutation is required for each distinct size.

The descriptor dimensions in Table 2 also permit a concrete feature-storage estimate. When stored as MATLAB double arrays (8 bytes per element), a single clear or encrypted feature vector requires 32 bytes for LTP, 184 bytes for oBIFs, 3.2 kB for RLD, and 216 bytes for LTP+oBIFs; combined representations require 64 bytes, 368 bytes, 6.4 kB, and 432 bytes, respectively. These values exclude MATLAB array metadata and the training-pair matrix. The latter can be substantially larger because all genuine-genuine and genuine-forgery dissimilarity vectors are retained. Empirical per-image runtime and peak memory were not logged in the original experiments, so the manuscript reports these algorithmic and representation-level bounds rather than reconstructing hardware measurements retrospectively. Relative to the clear descriptor-only baseline, encrypted adds the Josephus permutation step, whereas combined computes both clear and encrypted descriptors and doubles the representation dimension. Because empirical timing was not logged, no retrospective real-time claim is made.

5. RESULTS AND DISCUSSION

5.1. GPDS300

The full GPDS300 ablation results are summarized in Table 3. Combined LTP+oBIFs produced the best observed point estimate, with 85.06% ACC and 14.94% AER. Clear LTP was close at 84.91% ACC, whereas its encrypted version decreased to 77.45%. oBIFs was most strongly affected by encryption: ACC fell from 65.35% in the clear condition to 36.50% in the encrypted condition. Combined oBIFs recovered part of this loss but remained below the best LTP-based configurations. RLD changed only modestly between clear and combined.

5.2. SigComp 2011

The Dutch subset favored clear oBIFs, which achieved 98.08% ACC and 1.92% AER (Table 4). Encrypted LTP improved over clear LTP (97.51% versus 96.15% ACC), and combined RLD slightly exceeded clear RLD. In contrast, encryption reduced oBIFs and LTP+oBIFs performance. The Chinese subset was led by clear LTP+oBIFs at 88.58% ACC and 11.42% AER, followed closely by clear oBIFs at 88.50%. Most encrypted configurations were weaker. Combined RLD improved over its clear and encrypted forms, but its absolute performance remained lower than the clear local-texture descriptors.

Table 3. GPDS300 results, with bold indicating the overall best observed descriptor-condition point estimate

Descriptor	Condition	FAR (%)	FRR (%)	AER (%)	ACC (%)
LTP	Clear	11.24	18.93	15.09	84.91
LTP	Encrypted	25.26	19.84	22.55	77.45
LTP	Combined	21.4	16.14	18.77	81.23
oBIFs	Clear	24.95	44.35	34.65	65.35
oBIFs	Encrypted	57.15	69.85	63.5	36.5
oBIFs	Combined	38.13	27.61	32.87	67.13
RLD	Clear	22.11	28.49	25.3	74.7
RLD	Encrypted	24.26	37.94	31.1	68.9
RLD	Combined	18.83	32.07	25.45	74.55
LTP+oBIFs	Clear	19.02	12.68	15.85	84.15
LTP+oBIFs	Encrypted	24.7	34.1	29.4	70.6
LTP+oBIFs	Combined	11.06	18.82	14.94	85.06

Table 4. SigComp 2011 results, with bold indicating the overall best observed result within each dataset

Dataset	Descriptor	Condition	FAR	FRR	AER	ACC
Dutch	LTP	Clear	3.88	3.81	3.85	96.15
Dutch	LTP	Encrypted	2.45	2.53	2.49	97.51
Dutch	LTP	Combined	2.76	2.68	2.72	97.28
Dutch	oBIFs	Clear	1.94	1.9	1.92	98.08
Dutch	oBIFs	Encrypted	14.73	15.14	14.94	85.06
Dutch	oBIFs	Combined	6.55	6.36	6.46	93.54
Dutch	RLD	Clear	9.76	11	10.38	89.62
Dutch	RLD	Encrypted	17.31	19.53	18.42	81.58
Dutch	RLD	Combined	12.56	6.76	9.66	90.34
Dutch	LTP+oBIFs	Clear	3.38	1.38	2.38	97.62
Dutch	LTP+oBIFs	Encrypted	9.24	7.24	8.24	91.76
Dutch	LTP+oBIFs	Combined	5.15	3.15	4.15	95.85
Chinese	LTP	Clear	8.21	16.43	12.32	87.68
Chinese	LTP	Encrypted	10.27	20.33	15.3	84.7
Chinese	LTP	Combined	8.83	17.45	13.14	86.86
Chinese	oBIFs	Clear	7.8	15.2	11.5	88.5
Chinese	oBIFs	Encrypted	21.15	42.09	31.62	68.38
Chinese	oBIFs	Combined	19.1	38.19	28.65	71.35
Chinese	RLD	Clear	33.73	24.43	29.08	70.92
Chinese	RLD	Encrypted	33.2	33.2	33.2	66.8
Chinese	RLD	Combined	31.47	22.79	27.13	72.87
Chinese	LTP+oBIFs	Clear	10.42	12.42	11.42	88.58
Chinese	LTP+oBIFs	Encrypted	33.8	13.8	23.8	76.2
Chinese	LTP+oBIFs	Combined	20.4	20.4	20.4	79.6

5.3. SigWIcomp 2015

Table 5 reports score-based results. For Bengali, the lowest $\hat{C}_{llr}$ was 0.9485 with encrypted oBIFs, while the lowest $\hat{C}_{llr}^{min}$ was 0.0346 with combined RLD. For Italian, combined LTP+oBIFs achieved both the lowest $\hat{C}_{llr}$ (0.9238) and the lowest $\hat{C}_{llr}^{min}$ (0.0227). The clear LTP+oBIFs Italian result also had a low $\hat{C}_{llr}^{min}$ of 0.0264, indicating that most of the minimum-cost advantage was already present before adding the encrypted representation.

Figure 3 provides a direct visual comparison of the three datasets for which ACC/AER is the common reporting scale. The plot is descriptive rather than a replacement for the tables, and SigWIcomp 2015 is intentionally omitted because its score-based Cllr measures are not numerically commensurate with ACC.

5.4. Statistical uncertainty of the GPDS300 point estimates

The experiments use fixed partitions and were executed once, so split-to-split variance cannot be recovered from the aggregate manuscript results. Nevertheless, GPDS300 has known question counts: 150 test writers provide 4,500 forged and 1,800 genuine questions. As a descriptive question-level check, 95% Wilson confidence intervals for the best observed combined LTP+oBIFs configuration are approximately 10.18–12.01% for FAR and 17.08–20.69% for FRR. A first-order propagation of these binomial uncertainties gives an approximate AER interval of 13.93–15.95%. For clear LTP, the corresponding approximate AER interval is 14.07–16.10%. The overlap reinforces an important interpretation: the 14.94% versus 15.09% AER difference should be treated as a small difference in observed point estimates, not as evidence of statistical superiority. These intervals do not model writer-level clustering or alternative train/test partitions; repeated writer-level experiments would be required for that stronger inference. Because only one fixed-partition execution is archived, paired t-tests or ANOVA cannot be reconstructed validly and are therefore not reported.

Table 5. SigWIcomp 2015 results, with minimum values highlighted independently for each metric and dataset

Dataset	Descriptor	Condition	$\hat{C}_{llr}$	$\hat{C}_{llr}^{min}$
Bengali	RLD	Clear	1.0098	0.0397
Bengali	RLD	Encrypted	1.1157	0.4521
Bengali	RLD	Combined	1.0604	0.0346
Bengali	LTP	Clear	1.1652	0.0699
Bengali	LTP	Encrypted	1.0996	0.4131
Bengali	LTP	Combined	1.1319	0.0413
Bengali	oBIFs	Clear	1.4776	0.9755
Bengali	oBIFs	Encrypted	0.9485	0.4179
Bengali	oBIFs	Combined	0.9755	0.7481
Bengali	LTP+oBIFs	Clear	1.1166	0.1966
Bengali	LTP+oBIFs	Encrypted	1.0483	0.3986
Bengali	LTP+oBIFs	Combined	1.0816	0.2263
Italian	RLD	Clear	1.0118	0.8825
Italian	RLD	Encrypted	1.1282	0.9302
Italian	RLD	Combined	1.0617	0.8706
Italian	LTP	Clear	1.1603	0.904
Italian	LTP	Encrypted	1.1551	0.9267
Italian	LTP	Combined	1.1577	0.9112
Italian	oBIFs	Clear	1.0871	0.9082
Italian	oBIFs	Encrypted	1.0241	0.9418
Italian	oBIFs	Combined	0.9489	0.889
Italian	LTP+oBIFs	Clear	1.0559	0.0264
Italian	LTP+oBIFs	Encrypted	1.0885	0.4537
Italian	LTP+oBIFs	Combined	0.9238	0.0227

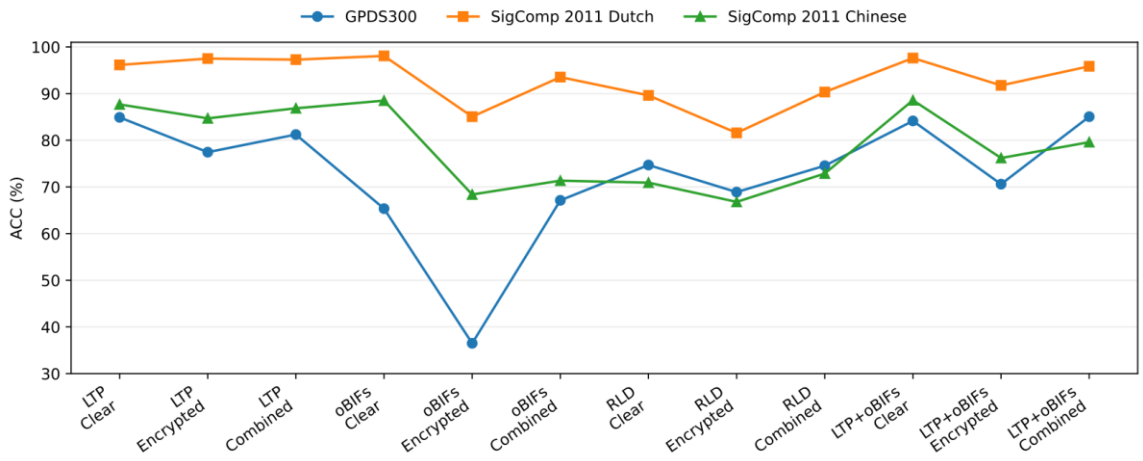


Figure 3. ACC comparison for GPDS300 and SigComp 2011, highlighting oBIFs degradation after Josephus rearrangement and dataset-dependent combined performance

5.5. Descriptor effects

The ablation supports the central hypothesis: Josephus encryption is not a generally improving preprocessing step. Its effect depends on the descriptor. oBIFs is the clearest example. The clear form was the best Dutch representation and nearly the best Chinese representation, whereas encrypted oBIFs produced large losses in both subsets and on GPDS300. This behavior is consistent with the descriptor design: oBIFs relies on local derivative responses and quantized orientation, and a global pixel rearrangement breaks coherent lines, edges, and ridge neighborhoods.

LTP showed a more mixed response. Encrypted LTP improved the Dutch result, suggesting that redistributed local contrasts supplied a useful alternative texture histogram for this subset. The same change was harmful on GPDS300 and Chinese signatures. Combined LTP did not consistently outperform both single representations, which indicates that simple concatenation can preserve redundant or noisy components as well as complementary ones.

RLD also exhibited selective complementarity. Combined RLD slightly improved the Dutch and Chinese ACC values relative to clear RLD and produced the lowest Bengali $\hat{C}_{llr}^{min}$. The transformation destroys original pen-stroke runs, but the resulting fragmentation and density distribution can still distinguish genuine

and forged samples in some datasets. The effect is modest rather than universal, and RLD remained below the best local-texture configurations on SigComp 2011.

The LTP+oBIFs combination was most effective on GPDS300 and Chinese signatures in the clear or combined condition. On GPDS300, adding the encrypted vector to the clear descriptor yielded the overall best point estimate, although the gain over clear LTP was small and not established as statistically significant. On Italian SigWIcomp, combined LTP+oBIFs produced the lowest values for both score metrics. These cases show that the encrypted representation can be useful when its additional components complement a strong clear descriptor, but the improvement must be demonstrated dataset by dataset. This descriptor-dependent performance variation is itself a key finding: cryptographic-style image rearrangement should be paired with a descriptor only after checking whether the transform preserves or destroys the spatial evidence on which that descriptor relies.

For future descriptor design, the results suggest a preservation test before feature fusion: descriptors that depend strongly on coherent local orientation should not be expected to benefit from an unrestricted global permutation, whereas histogram-based descriptors that summarize local contrast or fragmentation may occasionally gain complementary statistics. A more principled extension would therefore select or weight transformed features according to the invariances of the descriptor rather than concatenating clear and encrypted vectors by default.

5.6. Cross-script behavior and generalization

The best-performing configuration varied across subsets: clear oBIFs performed best for Dutch signatures, clear LTP+oBIFs for Chinese signatures, combined LTP+oBIFs for GPDS300, combined RLD for Bengali according to $\hat{C}_{llr}^{min}$, and combined LTP+oBIFs for Italian. This variability argues against a single script-independent descriptor-encryption rule. Differences in stroke continuity, local orientation concentration, writing density, reference availability, forgery production, and competition protocol all contribute to the observed outcomes.

Accordingly, the cross-script findings support only conditional transfer and should not be taken as evidence of universally transferable behavior. The five retained subsets include Latin, Chinese, and Bengali scripts, but they do not cover the full diversity of writing systems, acquisition devices, image degradations, or signer populations. Generalization to larger corpora or other scripts such as Arabic or Devanagari remains an empirical question. A practical system should validate descriptor and representation choices on development data representative of the intended signing population instead of automatically concatenating clear and encrypted features. This validation requirement is especially relevant to multilingual financial services, e-government identity checks, and academic credential verification, where signatures from different writing conventions may share the same authentication backend.

5.7. Protocol-aware comparison with learned representations

Modern learned representations provide an important performance context, but the published protocols are not directly interchangeable with the present ablation. For example, Hafemann *et al.* [14] achieved an EER of 1.72% on GPDS-160 with a CNN-based representation, but their development/exploitation protocol and evaluation metric differ from those used in this study. TransOSV [18], by contrast, reported transformer-based experiments on BHSig-H, BHSig-B, GPDS Synthetic, and CS749, none of which corresponds exactly to the five subsets retained in the present evaluation. Ruiz *et al.* [22] used Siamese networks and synthetic signatures in a writer-independent random-forgery setting, including cross-dataset tests involving SigComp11. These studies demonstrate the strength of learned representations, but their dataset subsets, forgery assumptions, training objectives, and metrics preclude a valid numerical ranking against Tables 3–5.

Accordingly, this article does not claim state-of-the-art verification performance against CNN or transformer systems. Its contribution is a controlled descriptor-level ablation in which the classifier, normalization, pair-generation rule, and template construction are held fixed while only the representation condition changes. A direct learned-baseline experiment under exactly the same writer partitions, questions, and metrics would be valuable future work and is necessary before drawing conclusions about absolute competitiveness.

5.8. Limitations and robustness scope

The study has several limitations. First, the experiments use fixed writer partitions and a single execution, so variability across alternative splits is not measured; the GPDS300 intervals above are only question-level descriptive approximations. Second, no controlled degradation experiment was performed for blur, additive noise, compression, low contrast, scanning artifacts, or adversarial perturbations. The reported results therefore establish performance only on the supplied benchmark images and should not be interpreted as evidence of robustness to degraded acquisition. Third, empirical runtime and peak memory were not

recorded; subsection 4.6 provides theoretical complexity and representation-storage estimates instead. Fourth, a deep CNN or transformer baseline was not rerun under the identical partitions and metrics, so cross-method comparisons remain protocol-aware literature context rather than a controlled benchmark. Fifth, s and k are fixed and not optimized, and the sensitivity of the representation to these parameters is unknown. Finally, Josephus encryption was assessed only through signature-verification performance and was not subjected to cryptographic security analysis.

6. CONCLUSION

This article examined Josephus encryption as a descriptor-dependent representation transform for cross-script offline signature verification. Its key contribution is a systematic descriptor-dependent evaluation of the same Josephus rearrangement across multiple scripts under a fixed writer-independent verification pipeline. Under a fixed writer-independent SVM pipeline, clear, encrypted, and combined LTP, oBIFs, RLD, and LTP+oBIFs representations produced different outcomes across GPDS300, SigComp 2011, and SigWIcomp 2015. The strongest observed results were not associated with one universal condition: combined LTP+oBIFs led GPDS300 and Italian SigWIcomp, clear oBIFs led Dutch SigComp, clear LTP+oBIFs led Chinese SigComp, and combined RLD gave the lowest Bengali minimum cost. The central conclusion is therefore selective rather than absolute. Josephus encryption can add useful evidence for particular descriptor-dataset pairs, but it can also remove the orientation and neighborhood structures on which a descriptor depends. The reusable lesson is that an encryption-based representation transform should be evaluated against the invariances and spatial dependencies of the downstream descriptor before feature fusion. Future work should examine repeated writer partitions, writer-level statistical uncertainty, controlled image degradations, s/k sensitivity, optimized permutation data structures, and CNN or transformer baselines evaluated under exactly the same partitions and metrics. Additional extensions include online signatures, multimodal biometric combinations such as handwriting with keystroke dynamics, and auditable ledger or blockchain-based authentication where these technologies are appropriate to the application.

ACKNOWLEDGMENTS

The authors have no additional acknowledgments to report. This research received no research grant or contract.

FUNDING INFORMATION

This research received no research grant or contract from any funding agency in the public, commercial, or not-for-profit sectors.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ismail Hadjadj	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓			
Abdeljalil Gattal	✓	✓					✓			✓		✓	✓	
Mouloud Ayad						✓				✓		✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

No new dataset was generated for this study. All benchmark data originated from the repositories or competition providers responsible for the respective datasets. The corresponding author can provide the MATLAB implementation, extracted features, and fixed train/test assignment files on reasonable request, to support reproduction and extension of the reported descriptor-encryption pipeline.

REFERENCES

[1] R. Plamondon and S. N. Srihari, "Online and off-line handwriting recognition: a comprehensive survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 1, pp. 63–84, 2000, doi: 10.1109/34.824821.

[2] D. Impedovo and G. Pirlo, "Automatic Signature Verification: The State of the Art," *IEEE Trans. Syst. Man, Cybern. Part C (Applications Rev.*, vol. 38, no. 5, pp. 609–635, Sep. 2008, doi: 10.1109/TSMCC.2008.923866.

[3] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Offline handwritten signature verification — Literature review," in *2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA)*, IEEE, Nov. 2017, pp. 1–8, doi: 10.1109/IPTA.2017.8310112.

[4] M. M. Hameed, R. Ahmad, M. L. M. Kiah, and G. Murtaza, "Machine learning-based offline signature verification systems: A systematic review," *Signal Process. Image Commun.*, vol. 93, p. 116139, Apr. 2021, doi: 10.1016/j.image.2021.116139.

[5] A. Singla and A. Mittal, "Exploring offline signature verification techniques: a survey based on methods and future directions," *Multimed. Tools Appl.*, vol. 84, no. 6, pp. 2835–2875, Nov. 2024, doi: 10.1007/s11042-024-20454-x.

[6] S. N. Srihari, A. Xu, and M. K. Kalera, "Learning Strategies and Classification Methods for Off-Line Signature Verification," in *Ninth International Workshop on Frontiers in Handwriting Recognition*, IEEE, pp. 161–166, doi: 10.1109/IWFHR.2004.61.

[7] E. J. R. Justino, F. Bortolozzi, and R. Sabourin, "Off-line signature verification using HMM for random, simple and skilled forgeries," in *Proceedings of Sixth International Conference on Document Analysis and Recognition*, IEEE, 2001, pp. 1031–1034, doi: 10.1109/ICDAR.2001.953942.

[8] Y. Guerbai, Y. Chibani, and B. Hadjadji, "The effective use of the one-class SVM classifier for handwritten signature verification based on writer-independent parameters," *Pattern Recognit.*, vol. 48, no. 1, pp. 103–113, Jan. 2015, doi: 10.1016/j.patcog.2014.07.016.

[9] Y. Serdouk, H. Nemmour, and Y. Chibani, "New off-line Handwritten Signature Verification method based on Artificial Immune Recognition System," *Expert Syst. Appl.*, vol. 51, pp. 186–194, Jun. 2016, doi: 10.1016/j.eswa.2016.01.001.

[10] E. N. Zois, L. Alewijnse, and G. Economou, "Offline signature verification and quality characterization using poset-oriented grid features," *Pattern Recognit.*, vol. 54, pp. 162–177, Jun. 2016, doi: 10.1016/j.patcog.2016.01.009.

[11] W. Bouamra, C. Djeddi, B. Nini, M. Diaz, and I. Siddiqi, "Towards the design of an offline signature verifier based on a small number of genuine samples for training," *Expert Syst. Appl.*, vol. 107, pp. 182–195, Oct. 2018, doi: 10.1016/j.eswa.2018.04.035.

[12] I. Hadjadj, A. Gattal, C. Djeddi, M. Ayad, I. Siddiqi, and F. Abass, "Offline Signature Verification Using Textural Descriptors," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019, pp. 177–188, doi: 10.1007/978-3-030-31321-0_16.

[13] A. Soleimani, B. N. Araabi, and K. Fouladi, "Deep Multitask Metric Learning for Offline Signature Verification," *Pattern Recognit. Lett.*, vol. 80, pp. 84–90, Sep. 2016, doi: 10.1016/j.patrec.2016.05.023.

[14] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Learning features for offline handwritten signature verification using deep convolutional neural networks," *Pattern Recognit.*, vol. 70, pp. 163–176, Oct. 2017, doi: 10.1016/j.patcog.2017.05.012.

[15] H. Rantzsch, H. Yang, and C. Meinel, "Signature embedding: Writer independent offline signature verification with deep metric learning," in *Advances in Visual Computing*, vol. LNCS 10073, 2016, pp. 616–625, doi: 10.1007/978-3-319-50832-0_60.

[16] D. Tsourounis, I. Theodorakopoulos, E. N. Zois, and G. Economou, "From text to signatures: Knowledge transfer for efficient deep feature learning in offline signature verification," *Expert Syst. Appl.*, vol. 189, p. 116136, Mar. 2022, doi: 10.1016/j.eswa.2021.116136.

[17] S. Roy, D. Sarkar, S. Malakar, and R. Sarkar, "Offline signature verification system: a graph neural network based approach," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 7, pp. 8219–8229, Jul. 2023, doi: 10.1007/s12652-021-03592-0.

[18] H. Li, P. Wei, Z. Ma, C. Li, and N. Zheng, "TransOSV: Offline Signature Verification with Transformers," *Pattern Recognit.*, vol. 145, p. 109882, Jan. 2024, doi: 10.1016/j.patcog.2023.109882.

[19] F. M. Alsuhimat and F. S. Mohamad, "A Hybrid Method of Feature Extraction for Signatures Verification Using CNN and HOG a Multi-Classification Approach," *IEEE Access*, vol. 11, pp. 21873–21882, 2023, doi: 10.1109/ACCESS.2023.3252022.

[20] N. Arab, H. Nemmour, M. L. Bouibed, and Y. Chibani, "1D-GAN for improving offline handwritten signature verification based on small sets of real samples," *Multimed. Tools Appl.*, vol. 84, no. 21, pp. 24541–24561, Jan. 2025, doi: 10.1007/s11042-024-20517-z.

[21] W. Xiao and H. Wu, "Learning features for offline handwritten signature verification using spatial transformer network," *Sci. Rep.*, vol. 15, no. 9453, Mar. 2025, doi: 10.1038/s41598-025-92704-3.

[22] V. Ruiz, I. Linares, A. Sanchez, and J. F. Velez, "Off-line handwritten signature verification using compositional synthetic generation of signatures and Siamese Neural Networks," *Neurocomputing*, vol. 374, pp. 30–41, Jan. 2020, doi: 10.1016/j.neucom.2019.09.041.

[23] S. D. Bhavani and R. K. Bharathi, "A multi-dimensional review on handwritten signature verification: strengths and gaps," *Multimed. Tools Appl.*, vol. 83, no. 1, pp. 2853–2894, Jan. 2024, doi: 10.1007/s11042-023-15357-2.

[24] K. Matsuda, W. Ohyama, and T. Wakabayashi, "Multilingual-Signature Verification by Verifier Fusion Using Random Forests," in *2017 4th IAPR Asian Conf. Pattern Recognit. (ACPR)*, IEEE, Nov. 2017, pp. 941–946, doi: 10.1109/ACPR.2017.156.

[25] A. Das, M. A. Ferrer, U. Pal, S. Pal, M. Diaz, and M. Blumenstein, "Multi-script versus single-script scenarios in automatic off-line signature verification," *IET Biometrics*, vol. 5, no. 4, pp. 305–313, Dec. 2016, doi: 10.1049/iet-bmt.2016.0010.

[26] M. Liwicki *et al.*, "Signature Verification Competition for Online and Offline Skilled Forgeries (SigComp2011)," in *Proc. 2011 Int. Conf. Doc. Anal. Recognit. (ICDAR)*, IEEE, Sep. 2011, pp. 1480–1484, doi: 10.1109/ICDAR.2011.294.

[27] M. I. Malik *et al.*, "ICDAR2015 competition on signature verification and writer identification for on- and off-line skilled forgeries (SigWIcomp2015)," in *Proc. 2015 13th Int. Conf. Doc. Anal. Recognit. (ICDAR)*, IEEE, Aug. 2015, pp. 1186–1190, doi: 10.1109/ICDAR.2015.7333948.

[28] L. Halbeisen and N. Hungerbühler, "The josephus problem," *J. Theor. des Nombres Bordeaux*, vol. 9, no. 2, pp. 303–318, 1997, doi: 10.5802/jtnb.204.

[29] Z. Hua, B. Xu, F. Jin, and H. Huang, "Image Encryption Using Josephus Problem and Filtering Diffusion," *IEEE Access*, vol. 7, pp. 8660–8674, 2019, doi: 10.1109/ACCESS.2018.2890116.
[30] X. Wang, X. Zhu, and Y. Zhang, "An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map," *IEEE Access*, vol. 6, pp. 23733–23746, 2018, doi: 10.1109/ACCESS.2018.2805847.
[31] X. Tan and B. Triggs, "Enhanced Local Texture Feature Sets for Face Recognition Under Difficult Lighting Conditions," *IEEE Trans. Image Process.*, vol. 19, no. 6, pp. 1635–1650, Jun. 2010, doi: 10.1109/TIP.2010.2042645.
[32] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 7, pp. 971–987, Jul. 2002, doi: 10.1109/TPAMI.2002.1017623.
[33] L. D. Griffin and M. Lillholm, "Symmetry Sensitivities of Derivative-of-Gaussian Filters," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 6, pp. 1072–1083, Jun. 2010, doi: 10.1109/TPAMI.2009.91.
[34] L. D. Griffin, M. Lillholm, M. Crosier, and J. Van Sande, "Basic image features (BIFs) arising from approximate symmetry type," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009, pp. 343–355, doi: 10.1007/978-3-642-02256-2_29.
[35] F. Vargas, M. Ferrer, C. Travieso, and J. Alonso, "Off-line Handwritten Signature GPDS-960 Corpus," in *Proc. 2007 9th Int. Conf. Doc. Anal. Recognit. (ICDAR)*, IEEE, Sep. 2007, pp. 764–768, doi: 10.1109/ICDAR.2007.4377018.
[36] C. Cortes and V. Vapnik, "Support-vector networks," *Mach. Learn.*, vol. 20, no. 3, pp. 273–297, Sep. 1995, doi: 10.1007/BF00994018.
[37] N. Brümmer and J. du Preez, "Application-independent evaluation of speaker detection," *Comput. Speech Lang.*, vol. 20, no. 2–3, pp. 230–275, Apr. 2006, doi: 10.1016/j.csl.2005.08.001.
[38] D. A. van Leeuwen and N. Brümmer, "An Introduction to Application-Independent Evaluation of Speaker Recognition Systems," in *Speaker Classification I*, 2007, pp. 330–353, doi: 10.1007/978-3-540-74200-5_19.

BIOGRAPHIES OF AUTHORS



Ismail Hadjadj conducts computer science research at the Laboratoire d'Informatique et de Mathématique, Faculty of Exact Sciences, University of Bouira, and at the Laboratoire de Vision et d'Intelligence Artificielle, Echahid Cheikh Larbi Tebessi University, Tébessa, Algeria. His research focuses on offline handwritten signatures and handwriting, with related interests in biometrics, pattern recognition, image analysis, feature engineering, classification, and machine learning. His previous publications include work on textural representations for signature verification and encryption-based handwriting recognition. In this study, his contributions covered conceptualization, methodology, software development, validation, formal analysis, investigation, data curation, original draft preparation, manuscript review and editing, and visualization. He can be contacted at email: i.hedjadj@univ-bouira.dz.



Abdeljalil Gattal is a full professor of computer science at the University of Tebessa, Algeria, where he also leads a research team within the Laboratoire de Vision et d'Intelligence Artificielle (LAVIA). He earned a B.S. in Computer Science from the University of Skikda in 2004, followed by an M.S. in Information and Knowledge Systems from Abbes Laghrour University of Khenchela in 2009. In 2016, he completed a Ph.D. in Computer Science at the Ecole Nationale Supérieure d'Informatique, with research centered on segmentation and verification for handwritten digit recognition. His current research addresses image analysis, pattern recognition, and handwriting recognition. For this article, he contributed to conceptualization, methodology, resources, manuscript review and editing, supervision, and project administration. He can be contacted at email: abdeljalil.gattal@univ-tebessa.dz.



Mouloud Ayad is an assistant professor in the Department of Electronics at Sétif 1 University and a member of its LIS Laboratory. His academic training in electronics was completed at Sétif 1 University (Ferhat Abbas University), where he obtained engineering, Magister, and Ph.D. degrees in 2001, 2005, and 2015, respectively. His research interests encompass signal processing, microwave circuit design, microstrip technologies, and waveguide structures. His contributions to the present work were investigation, supervision, and manuscript review and editing. He can be contacted at email: m.ayad@univ-setif.dz.