Blind Watermarking of Online Handwritten Signals Based on DCT

Marcos Faundez-Zanuy
Tecnocampus, Universitat Pompeu Fabra
Mataró (Barcelona), Spain
faundez@tecnocampus.cat

***Abstract*—This paper presents a novel blind watermarking scheme for online handwritten signatures using the Discrete Cosine Transform (DCT). The proposed method embeds imperceptible watermarks into the high-frequency components of handwriting signals while preserving biometric recognition performance. Experimental results on the MCYT signature dataset show that the approach does not degrade recognition accuracy when embedding a 40-bit watermark (20 bits in the x-coordinate and 20 in the y-coordinate). This 40-bit capacity is sufficient to encode a timestamp, allowing the system to trace the time of signature creation. Despite these modifications, the watermark remains detectable, and signature recognition remains effective. Furthermore, the embedded timestamp provides a mechanism for detecting replay attacks, enhancing security in biometric authentication systems.**

***Index Terms*—biometrics, signature recognition, watermark, DCT**

I. Introduction

Watermarking is a well-established technique for embedding imperceptible information into signals, ensuring authenticity, copyright protection, and tamper detection [1] , [2]. In the context of online handwritten signals, watermarking plays a crucial role in preserving authorship and preventing unauthorized modifications. Among the various watermarking approaches, blind watermarking techniques stand out due to their ability to extract the embedded information without requiring the original unmarked signal. One effective approach for blind watermarking of online handwritten signals involves the Discrete Cosine Transform (DCT), which provides a robust and efficient means of embedding and extracting watermarks while maintaining signal integrity. Despite the extensive research on watermarking in multimedia content such as images, audio, and video, as well as its applications in biometric signals like fingerprints and iris recognition, the field of online handwritten signal watermarking remains significantly underexplored. The dynamic and sequential nature of handwriting signals presents unique challenges that differ from those encountered in traditional multimedia and biometric data. Consequently, there is a pressing need for more research to develop effective watermarking schemes tailored to the specific characteristics of online handwritten signals. To date, only a limited number of studies have addressed watermarking techniques for online handwriting. The existing literature includes [3], which investigates time-domain methods based on Least Significant Bit (LSB) modification and difference expansion, and [4], which explores non-blind watermarking techniques in the transform domain. These approaches provide foundational insights into the field, but there remains a gap in the development of robust blind watermarking methods, particularly those leveraging frequency-domain transformations like the DCT. This paper aims to bridge this gap by proposing a novel blind watermarking scheme for online handwritten signals using DCT, ensuring a balance between imperceptibility, robustness, and security.

This research was partly supported by the PID2023-146644OB-I00, funded by MICIU/AEI 10.13039/501100011033 and the European Union's FEDER program

A. Types of Watermarking

Watermarking methods can be broadly classified [5] into the following types based on various criteria:

- **Visible vs. Invisible Watermarking**: Visible watermarking embeds perceptible information, such as logos or text, directly onto the signal, whereas invisible watermarking ensures that the embedded information remains imperceptible under normal conditions.
- **Robust vs. Fragile Watermarking**: Robust watermarking is designed to withstand signal processing operations such as compression, filtering, and noise addition. In contrast, fragile watermarking is sensitive to modifications and is primarily used for tamper detection.
- **Blind vs. Non-Blind Watermarking**: Blind watermarking does not require access to the original unmarked signal for extraction, making it highly suitable for real-world applications. Non-blind watermarking, on the other hand, requires the original signal for verification.
- **Spatial vs. Transform Domain Watermarking**: Spatial domain watermarking embeds information directly into the signal samples, whereas transform domain techniques, such as those based on DCT, embed the watermark in the frequency coefficients, enhancing robustness against various attacks.

By leveraging DCT-based blind watermarking techniques, it is possible to embed imperceptible yet resilient watermarks into online handwritten signals. The application of DCT allows for selective embedding in frequency components that are less susceptible to noise while preserving the essential characteristics of the handwriting. This method ensures a balance

between imperceptibility, robustness, and security, making it a promising approach for protecting digital handwriting data.

II. Blind DCT watermaking

Blind watermarking using the Discrete Cosine Transform (DCT) involves embedding information into a signal in such a way that the original unmarked signal is not required for extraction. This ensures greater flexibility and practicality in real-world scenarios, where access to the original data may be limited or impractical. The proposed blind DCT-based watermarking technique consists of the following steps:

A. Watermark Embedding

The watermark embedding process is designed to integrate timestamp information into the Discrete Cosine Transform (DCT) domain of online handwritten signatures while maintaining signal integrity. The steps are as follows:

1) Apply the 1D DCT to the X and Y coordinate sequences of the online handwritten signal (1):

$$DCT_X = DCT(x), \quad DCT_Y = DCT(y) \tag{1}$$

2) Select an replace a subset of the DCT coefficients for embedding: In the blind approach, specific coefficients are fully replaced with the watermark values, which are scaled by a strength factor α (2):

$$C_w(i) = \alpha W(i), \quad \forall i \in S \tag{2}$$

where $C_w(i)$ represents the modified DCT coefficients, $W(i)$ is the watermark bit sequence, S is the set of selected coefficients for embedding, and α is the strength factor controlling the watermark's impact on the signal.

3) Apply the inverse DCT (IDCT) to reconstruct the watermarked signal (3):

$$(x_w, y_w) = \text{round}\left(\text{IDCT}(\text{DCT}(X, Y))\right) \tag{3}$$

where the rounding operator ensures that the samples remain integers.

Strengthening the watermark ($\alpha \uparrow$) enhances robustness against signal processing operations such as noise addition, compression, and resampling, making it more secure and easier to detect during extraction. However, increasing the strength also introduces greater distortion in the signal, which can negatively impact biometric recognition accuracy and reduce imperceptibility by making the watermark more detectable. This trade-off requires careful tuning of α to balance security and robustness with signal fidelity, ensuring the watermark remains both resilient and unobtrusive in practical applications. Figure 1 shows an example original signature (top), its watermarked version with strength $\alpha = 20$ (middle) and with strength $\alpha = 200$ (bottom). Although degradation is evident for large α values, the signature is still legible.

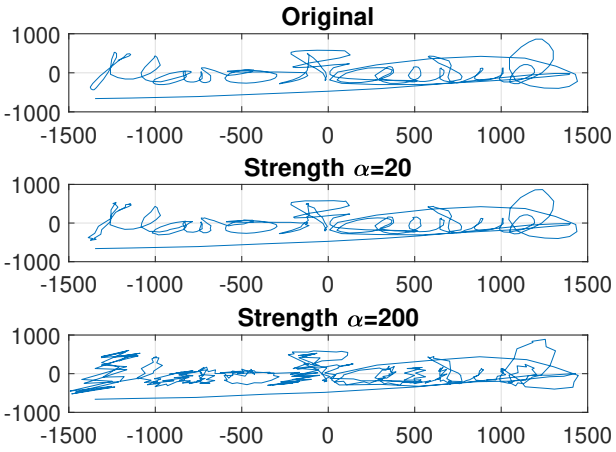

Fig. 1. Watermarked signatures with different strengths.

B. Watermark Extraction

The extraction process is blind, meaning the original signature is not required:

1) Apply the 1D DCT to the received watermarked signal:

$$DCT_{X_w} = DCT(x_w), \quad DCT_{Y_w} = DCT(y_w) \tag{4}$$

2) Extract the watermark bits from the predefined coefficient locations (5):

$$W'(i) = \begin{cases} 1 & \text{if } C_w(i) > \frac{\alpha}{2}, \\ 0 & \text{otherwise,} \end{cases} \quad \forall i \in S \tag{5}$$

Where:

- $W'(i)$ is the extracted bit at index i, which is either 1 or 0 depending on the comparison.
- $C_w(i)$ is the recovered DCT coefficient at index i (it can correspond to either the x- or y-related coefficients).
- α is the strength of the watermark, used as the threshold to decide the bit value.
- S is the set of indices being used for extraction.

The extraction process assigns a bit value of 1 if the recovered DCT coefficient exceeds half of the strength ($\alpha/2$), and 0 otherwise. This binary decision rule is applied for all indices $i \in S$.

3) In case of redundancy in the watermark, use error correction coding techniques to enhance the robustness of extracted watermark bits against noise and signal degradation.

This blind DCT-based approach ensures robustness against common signal processing operations such as noise addition, resampling, and minor transformations. Furthermore, by fully replacing selected DCT coefficients with watermark bits, the technique enables a straightforward and efficient extraction process without requiring access to the original unmarked signal. In Figure 2, we present the temporal evolution of the x-

and y-coordinates of the signature, along with their Discrete Cosine Transform (DCT) representations, for the user with the shortest signature in the database. We observe good energy compaction in the transform domain, with the highest values concentrated at the lowest frequencies.

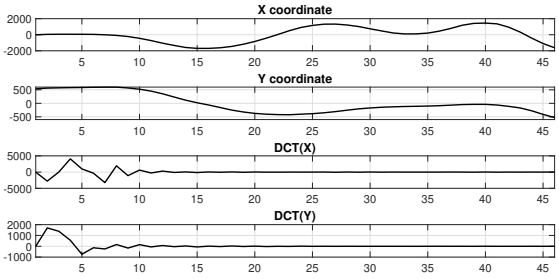

Fig. 2. Signature data representation: (top to bottom) x-coordinate, y-coordinate, DCT of the x-coordinate, and DCT of the y-coordinate for the user with the shortest signature in the database.

III. Materials and Methods

A. Database

For this study, we utilize the MCYT [6] signature dataset, which is a subset of the MCYT baseline corpus. This dataset is specifically designed for benchmarking online handwritten signature recognition and verification methods. Figure 3 displays a histogram of the signature lengths, providing insight into the variability within the dataset of 330 users. The minimum length is 46 samples, and the maximum length is 1798 samples.

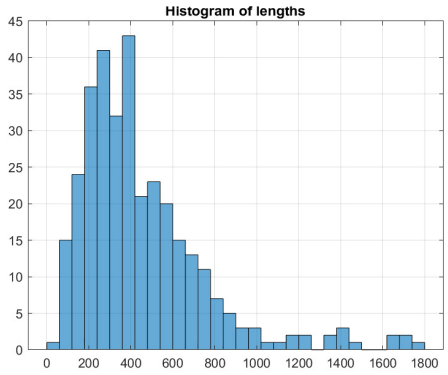

Fig. 3. Histogram of the lengths of user signatures. This figure shows the distribution of signature lengths for the dataset used in the watermarking experiment.

The key attributes of the dataset are as follows:

- **Data Collection:** The signatures were acquired using a WACOM Intuos A6 USB tablet. The device records both and spatial coordinates, the pressure (p) exerted by the pen, along with azimuth and altitude angles. The sampling rate is 100 Hz with a resolution of 2540 lines per inch.
- **Participants:** A total of 330 individuals contributed to the dataset.
- **Genuine Signatures:** Each participant provided 25 authentic signature samples.
- **Skilled Forgeries:** Additionally, each individual attempted 25 forgeries, mimicking genuine signatures with expertise.

B. Watermark content

We will use as watermark a timestamps with millisecond precision into binary representation. By converting timestamps into milliseconds since a reference epoch, we minimize storage requirements while maintaining high accuracy. Only 40 bits are required to represent timestamps ranging from the year 2000 to 2030, making this approach both space-efficient and computationally simple.

Timestamps play a crucial role in avoiding replay attacks [7], [8], [9]

To efficiently encode timestamps, we compute the total milliseconds elapsed from a chosen epoch (e.g., 2000-01-01 00:00:00.000). The formula used is (6):

$$T_{ms} = (Y-2000)\times 365.2425\times 24\times 60\times 60\times 1000+M_{ms} \quad (6)$$

where Y is the year, and M_{ms} accounts for the additional ms required to represent the full timestamp with millisecond precision.

To determine the required bit-length, we estimate the maximum number of milliseconds between 2000 and 2030:

$$(2030-2000)\times 365.2425\times 24\times 60\times 60\times 1000 \approx 9.567\times 10^{11} \quad (7)$$

Since $2^{39} = 5.497 \times 10^{11}$ and $2^{40} = 1.099 \times 10^{12}$, we conclude that 40 bits are sufficient.

This result is comparable to encoding individual components separately (see Table I):

TABLE I
Bits required for encoding different time components.

Component	Range	Bits Required
Year	2000-2030	5
Month	1-12	4
Day	1-31	5
Hour	0-23	5
Minute	0-59	6
Second	0-59	6
Millisecond	0-999	10

We analyzed the relationship between the length of the signature and the Mean Absolute Error (MAE) at the last insertion point of the watermark. As shown in Figure 4, the scatter plot illustrates how the length of each user's signature affects the MAE at the final insertion point. We observe that, the longer the signature, the smaller the distortion.

Finally, Figure 5 shows the performance of watermark insertion in terms of MAE across the entire dataset. The top part of the figure highlights the results for the shortest and longest user signatures (users 16 and 256, respectively), while the bottom part shows the MAE for all 330 users, providing a

comprehensive overview of the watermark insertion distortion. From this figure, we observe that to minimize distortion, the watermark should be inserted at the last samples of the signature.The watermark consists of 40 samples. The first 20 are inserted into the x-coordinate, and the remaining 20 are inserted into the y-coordinate.

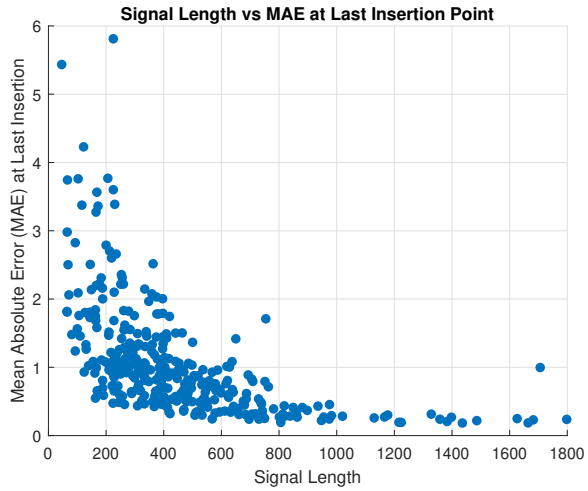

Fig. 4. Signal length vs. Mean Absolute Error (MAE) at the last insertion point. The scatter plot illustrates the relationship between the length of the signature and the MAE value at the final watermark insertion point for each user.

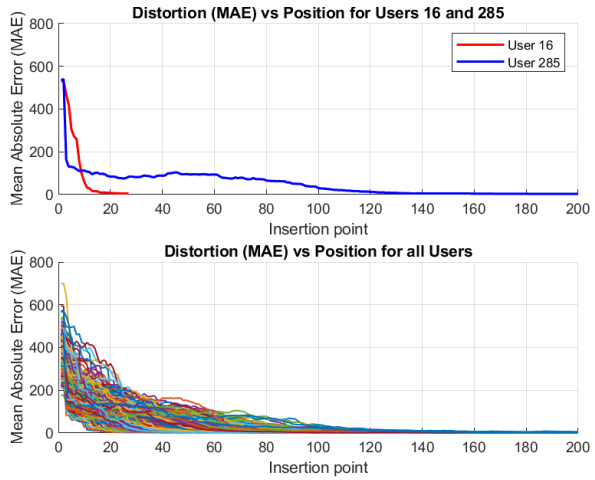

Fig. 5. MAE vs. insertion watermark point for the shortest and longest user signatures. The figure shows the MAE for users with the shortest and longest signatures on the top and the MAE for the entire dataset of 330 users on the bottom.

C. Recognition Algorithm

The recognition framework models each user based on a training set comprising five genuine signatures. For any test signature, the system calculates the Dynamic Time Warping (DTW) [10] distance against each of the five stored reference signatures. The final similarity score is determined as the minimum of these five computed distances.

Two operational modes are considered [11]:

- **Identification:** The DTW distance is computed for all N enrolled users. The model yielding the lowest distance is assigned as the recognized identity.
- **Verification:** The DTW distance is calculated between the test signature and the claimed identity model. If the computed distance falls below a pre-defined threshold, the signature is accepted as genuine; otherwise, it is classified as an impostor attempt. The threshold determination and verification accuracy assessment rely on the minimum detection cost function (minDCF) as described in [12].

D. Feature Extraction

To ensure consistency in analysis, the signature attributes—including and coordinates and pressure (p) values—are first standardized by normalizing them to zero mean and unit variance. Following normalization, dynamic features are derived from the first and second derivatives of the signature data. The extraction process is as follows:

First Derivative (Velocity)

The velocity components of the signature are obtained by computing the first derivative over a window of 11 points [13]. These represent the instantaneous rates of change of position and pressure (8):

$$\dot{x} = \frac{dx}{dt}, \quad \dot{y} = \frac{dy}{dt}, \quad \dot{p} = \frac{dp}{dt} \tag{8}$$

Second Derivative (Acceleration)

Acceleration components are computed as the second derivative of the signature trajectory (9):

$$\ddot{x} = \frac{d^2x}{dt^2}, \quad \ddot{y} = \frac{d^2y}{dt^2}, \quad \ddot{p} = \frac{d^2p}{dt^2} \tag{9}$$

Both velocity and acceleration values are subsequently normalized by subtracting their mean and dividing by their standard deviation. The final feature vector is then constructed as (10):

$$\mathbf{v}_n = [x_n, y_n, p_n, \dot{x}_n, \dot{y}_n, \dot{p}_n, \ddot{x}_n, \ddot{y}_n, \ddot{p}_n] \tag{10}$$

This vector is computed for each sampled point in the signature.

IV. Experimental Results

Table II presents the performance metrics obtained for different strength values. $\alpha = 1$ means that the removed DCT coefficients are directly replaced by watermark bits, while $\alpha = 0$ means that they are simply overwritten with zeros. The original recognition rates over the complete signal are represented in the first row with the "No watermark" indication. *minDCFr* represents the minimum detection cost function in verification for random forgeries, while *minDCFs* corresponds to the result for skilled forgeries.

TABLE II
PERFORMANCE METRICS FOR DIFFERENT STRENGTH LEVELS

Strength (α)	**IDR (%)**	**minDCFr (%)**	**minDCFs (%)**
No watermark	98.55	1.14	3.92
0	98.55	1.14	3.92
1	98.55	1.15	3.92
21	98.55	1.15	3.92
81	98.55	1.17	3.92
500	97.82	1.39	4.18
1000	97.82	2.09	4.44

Experimental results from Table II reveals a small degradation in recognition accuracy even for large α values.

These results are not surprising, as we are primarily watermarking the high-frequency content of the signal. High-frequency components tend to carry less perceptual significance and can often be altered without drastically affecting the overall structure of the signal. Even if the modified coefficients were removed, recognition could still be performed, as the essential discriminative features reside largely in the lower-frequency components. However, it is important to note that the experimental results shown in Table II do not involve such a removal process; rather, they reflect the direct impact of watermark embedding on recognition performance.

V. CONCLUSION

In this paper, we proposed a blind watermarking approach for online handwritten signatures based on DCT, embedding a timestamp to prevent replay attacks while preserving biometric recognition performance. The experimental results demonstrated that our method introduces only a small degradation in recognition accuracy for large α values. These results confirm that watermarking primarily affects the high-frequency content of the signal, leaving essential discriminative features intact. A key advantage of this method is its blind watermarking nature, meaning that watermark extraction does not require access to the original unmarked signature. This makes the approach more practical and flexible in real-world scenarios, where storing or retrieving the original signal may be impractical. Additionally, blind watermarking enhances scalability and usability, as it allows for authentication and replay attack prevention without the need for reference templates. This property is particularly valuable in remote authentication systems and cloud-based biometric applications, where efficient and secure verification is essential While this technique may not be highly robust against intentional removal attacks, it is effective in collaborative user scenarios where access control discourages malicious tampering. Furthermore, the use of timestamp embedding enhances security by providing protection against replay attacks. Future work could explore more adaptive watermarking strategies to further improve robustness while maintaining recognition accuracy.

A. Limitations

While the proposed watermarking approach may not be highly resistant to targeted removal attacks, this is not necessarily a critical limitation in a collaborative user scenario. In environments where access to a service can be denied based on watermark verification, there is little incentive for users to actively attack the watermark. Instead, the technique serves its intended purpose of embedding traceable information while maintaining recognition performance within acceptable limits. One common attack, such as rotation, can be mitigated through de-rotation normalization applied prior to recognition. As shown in [14], de-rotation does not significantly affect recognition accuracies, making it a viable preprocessing step to counteract such transformations without degrading system performance. However, it is important to consider that signatures captured using different acquisition devices may exhibit variations in quality or dynamics, potentially affecting the behavior of both watermarking and recognition systems.

REFERENCES

[1] D. Awasthi, A. Tiwari, P. Khare, and V. Kumar Srivastava, "A comprehensive review on optimization-based image watermarking techniques for copyright protection," *Expert Systems with Applications*, vol. 242, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417423033328

[2] A. Kumari, H. Madhukar, S. A. Haider, A. Majumder, and S. Kundu, *Digital watermarking strategies for healthcare data security: A comprehensive review and analysis*. IGI Global Scientific publishing, 2024, pp. 106–117. [Online]. Available: https://www.igi-global.com/chapter/digital-watermarking-strategies-for-healthcare-data-security/347581

[3] M. Faundez-Zanuy, "Comprehensive analysis of least significant bit and difference expansion watermarking algorithms for online signature signals," *Expert Systems with Applications*, vol. 267, p. 126214, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417424030811

[4] ——, "Online signature watermarking in the transform domain," *Cognitive Computation*, vol. 17, no. 2, p. 79, 2025. [Online]. Available: https://doi.org/10.1007/s12559-025-10436-y

[5] F. Petitcolas, R. Anderson, and M. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[6] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho *et al.*, "Mcyt baseline corpus: a bimodal biometric database," *IEE Proceedings-Vision, Image and Signal Processing*, vol. 150, no. 6, pp. 395–401, 2003.

[7] M. Faundez-Zanuy, M. Hagmüller, and G. Kubin, "Speaker verification security improvement by means of speech watermarking," *Speech Communication*, vol. 48, no. 12, pp. 1608–1619, 2006, nOLISP 2005. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167639306000653

[8] ——, "Speaker identification security improvement by means of speech watermarking," *Pattern Recognition*, vol. 40, no. 11, pp. 3027–3034, 2007. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S003132030700101X

[9] M. Faundez-Zanuy, J. J. Lucena-Molina, and M. Hagmüller, "Speech watermarking: an approach for the forensic analysis of digital telephonic recordings," *Journal of Forensic Sciences*, vol. 55, no. 4, pp. 1080–1087, Jul 2010, epub 2010 Apr 16.

[10] M. Faundez-Zanuy, "On-line signature recognition based on vq-dtw," *Pattern Recognition*, vol. 40, no. 3, pp. 981–992, 2007.

[11] ——, "Biometric security technology," *IEEE Aerospace and Electronic Systems Magazine*, vol. 21, no. 6, pp. 15–26, 2006.

[12] A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki, "The det curve in assessment of detection task performance," in *Proc. 5th European Conference on Speech Communication and Technology (Eurospeech 1997)*, 1997, pp. 1895–1898.

[13] M. Faundez-Zanuy and M. Diaz, "On the use of first and second derivative approximations for biometric online signature recognition," in *Advances in Computational Intelligence*, I. Rojas, G. Joya, and A. Catala, Eds. Cham: Springer Nature Switzerland, 2023, pp. 461–472.

[14] M. Faundez-Zanuy, "Analysis of inclinations in genuine signatures and skilled forgeries," in *Proceedings of the 22nd Conference of the International Graphonomics Society (IGS 2025)*, Polytechnique Montréal, Canada, June 2025, https://www.igs2025.org.