Jurnal Infotekmesin
Vol.12, No.02, Juli 2021
p-ISSN: 2087-1627, e-ISSN: 2685-9858
DOI: 10.35970/infotekmesin.v12i2.668, pp.155-159

An Enhanced Dynamic Signature Verification using the X and Y Histogram Features

Aris Tjahyanto[1*], Ano Rangga Rahardika[2] , Ary Mazharuddin Shiddiqi[3]
[1, 2]Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember
[3]Departemen Teknik Informatika, Institut Teknologi Sepuluh Nopember
[1,2,3]Kampus ITS Sukolilo, Surabaya, 60111, Indonesia
E-mail: aristj@its.ac.id[1], ano14@mhs.is.its.ac.id[2], ary.shiddiqi@if.its.ac.id[3]

Info Naskah:
Naskah masuk: 7 Mei 2021
Direvisi: 17 Agustus 2021
Diterima: 24 Agustus 2021

Abstrak

Verifikasi tanda tangan dinamis yang menggunakan fitur histogram adalah teknik deteksi pemalsuan tanda tangan yang terkenal karena performanya yang tinggi. Namun, teknik ini seringkali terbatas pada histogram sudut yang diturunkan dari vektor yang mengandung dua titik yang berdekatan. Kami mengusulkan tambahan fitur baru dari histogram X dan Y untuk mengatasi keterbatasan tersebut. Eksperimen kami menunjukkan bahwa teknik kami menghasilkan nilai Area Bawah Kurva (AUC) sebesar 0,80 untuk mendeteksi pemalsuan terlatih dan 0,91 untuk pemalsuan acak. Teknik kami bekerja paling baik saat sistem verifikasi menggunakan 12 fitur yang paling dominan. Pengaturan ini menghasilkan nilai AUC sebesar 0,80 untuk mendeteksi pemalsuan terlatih dan 0,93 untuk pemalsuan acak. Hasil ini mengungguli teknik sebelumnya ketika fitur histogram X dan Y tidak digunakan yang menghasilkan nilai AUC 0,78 untuk mendeteksi pemalsuan terlatih dan 0,90 untuk pemalsuan acak.

Keywords:
Dynamic Signature;
Histogram X;
Histogram Y;
Mobile Device;
AUC.

Abstract

Dynamic signature verification by using histogram features is a well-known signature forgery detection technique due to its high performance. However, this technique is often limited to angular histograms derived from vectors containing two adjacent points. We propose additional new features from the X and Y histograms to overcome the limitation. Our experiments indicate that our technique produced Under Curve Area AUC values 0.80 to detect skilled forgery and 0.91 for random forgery. Our method performed best when the verification system uses 12 of the most dominant features. This setup produced AUC values of 0.80 to detect skilled forgery and 0.93 for random forgery. These results outperformed the original technique when the X and Y histogram features are not used that produced AUC values of 0.78 to detect skilled forgery and 0.90 for random forgery.

***Penulis korespondensi:**
Aris Tjahyanto
E-mail: aristj@its.ac.id

1. Introduction

In the past decade, many studies investigated dynamic signature verification. A study conducted by Sae-Bae explored the histogram feature to verify online signatures [1]. The histogram is a common feature used for object recognition [2] [3], and offline signature recognition [4]. The use of histograms for online signatures was first introduced in [5]. The technique was enhanced using part of the histogram features, as demonstrated in [6] by scaling the histogram. But the use of histograms is only limited to angular histograms derived from vectors containing two adjacent points. According to [1], more information is available in dynamic signatures, which can be used to produce histogram features for online signature verification. They experimented by obtaining the histogram feature not only based on angles, but also based on changes in position, changes in position length, changes in speed, and periods of change in speed from dynamic signature data. They also form a two-dimensional histogram derived from a combination of two different variables. However, the results are not optimal because the histogram comes from ($X1, Y1, R1, \Phi1, X2, Y2, R2, \Phi2$).

We use additional features derived from X and Y histograms to detect signature forgery. We use the features considering the information about the distribution of positions in dynamic signatures the features carry. If the signature is different, the histogram distribution of the X and Y positions will also differ. Therefore, X and Y histograms can be robust for detecting cases of random forgery (RF) or skilled forgery (SF). The AUC (Area Under Curve) curve from the ROC (Receiver Operating Characteristic) was used to measure the signature verification system's performance. The ROC curve is a two-dimensional curve where the True Positive Rate (TPR) is plotted along the y-axis, and the False Positive Rate (FPR) is plotted along the x-axis, with several threshold points. We used 50 threshold points and plotted the curves based on the TPR and FPR values at each threshold value. The AUC value is interpreted as the probability of an original signature verified as authentic rather than a fake signature confirmed as authentic. In simple, higher true positive than false positive. The higher the AUC value, the better the classifier.

The AUC value of the ROC curve is used to compare the performance of two classifier systems. It is recommended to use the whole ROC rather than just one particular point when comparing two methods [7] [8]. The maximum value of AUC is 1, indicated by a triangle curve from the left end (0,1) and the right end (1,1). This situation occurs when there is no False Negative on each threshold. When AUC equal 0.5, a diagonal line of (0.0) and (0.1) is formed. This situation indicates a random verifier alias performance that only provides guesses in the case of binary classification. If the AUC value is below 0.5, then there is an error in the verification algorithm or an irrelevant feature because it is worse than a random guess. We compared the AUC value of the verification system with and without new features. We used the new features one at a time and then sorted the AUC values in descending order. Then, we grouped the new features into 4, 8, 12, 13, 14, and 15 categories.

2. Methods

The system is divided into two stages, namely the enrollment stage and the verification stage (Figure 1). Each stage consists of several processes. The enrollment stage consists of the process of lines concatenation, data derivation/reduction, feature extraction, and template matching. The verification stage consists of the process of line concatenation, data derivation/reduction, feature extraction, and Manhattan distance calculation.

We obtain signatures using the CoolpadR18 device through a Web application with HTML5 technology, including position x, position y, and time stamp. There are 19 people who gave their original signatures with 20 samples for each person. Some people are requested to imitate someone else's signature to simulate fake signatures. The original signatures were taken the same day, while three people imitate fake signatures the next day. Fake signatures are made by paying attention to the original signature and viewing the video recorded when making the original signature. All signatures are stored in a text file on the server for further processing. We used the library canvas to create signature data (https://github.com/szimek/signature_pad). We used a library property called "throttle" for setting when a

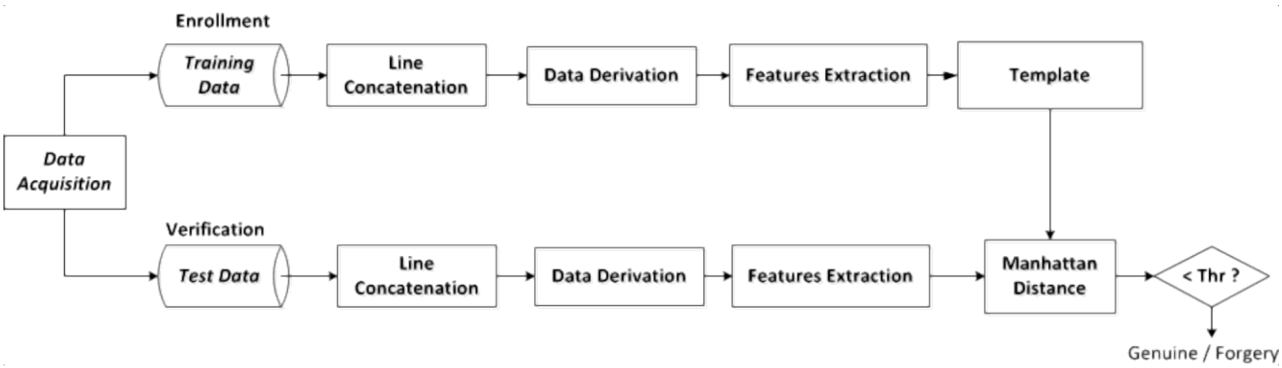


Figure 1. System Description

signature point is taken so that the time difference from one point to another is the same. This way, there we do not need interpolation to equalize the time difference.

Ten original signatures from each person were taken and used as training and testing data (190 original signatures each). There are two categories of forgery for testing: the skilled forgery (SF) and the random forgery (RF). SF testing data were produced ten times by viewing the video of writing original signatures. RF testing data were produced ten times without viewing the video of writing original signatures.

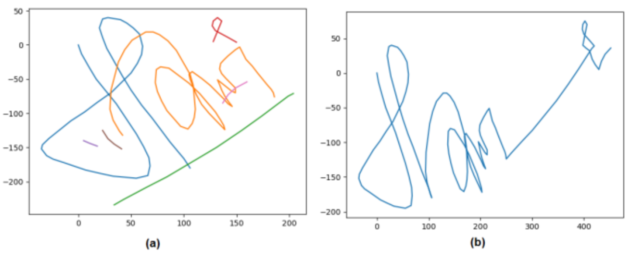


Figure 2. (a). Signature before line concatenation. (b) Signature after line concatenation

Figure 2 shows the process of lines concatenation. Lines concatenation is a process in the preprocessing step. The signature lines are put together first to overcome the problem of variations in the number of lines. For example, $S = \{s_1, s_2, ..., s_N\}$ are online signatures with normalized lines where each line S_i can be seen in Eq.(1).

$$s_i = \left\{(x_1^i, y_1^i), ..., (x_m^i, y_m^i)\right\} \quad (1)$$

Where S_i is a series of points (x_j, y_j) of length *m*. The following lines are combined by moving the origin of a line to the endpoint of the previous line. Then a dynamic signature is broken up into two-time series components (the time series x and y) denoted by X and Y. After the two signature components are combined, the next step is data derivation or data reduction. Data derivation is a step to get the invariant position of the signature. The derivation formula can be seen in [1] [9]. Before performing the derivation process, it is necessary to calculate implicit information from a signature, including the angle θ and r. The angle θ is formed in the coordinates (x, y), and r is the length of the line between the points (x, y) and the origin (0, 0). The set θ and r are denoted by Φ and R. So that the complete information obtained before the data derivation process is (X, Y, Φ, R). For details, the data derivation formula can be seen in [1].

After an implicit information vector is obtained from a signature, the vector will be passed down to the second level. For example, x^1_n data is calculated from $x^1_n = x_n - x_{(n-1)}$. Then, the level one derivation is (X^1, Y^1, Φ^1, R^1), while the level two derivation is (X^2, Y^2, Φ^2, R^2). This derivative vector is then used to extract the histogram feature in the next step.

A histogram is formed by dividing vector values, which are limited by min and max values , into bins with the same width. Then, the frequency of a bin is calculated from every element that falls into the bin's range. For this, we need information about the values of elements to construct a histogram. Vectors with integers such as X^1 are given eight bin numbers, whereas vectors with fractional values such as angles and line lengths are given more bin numbers. The finer the value of the vector, the more bins required. This method aims to capture small value differences and group it in a different bin to produce better features. For the angle vector Φ, a limit value of [-π, π] is given. For vectors that do not have an explicit limit, the minimum value is calculated from the average value minus three times the standard deviation. The maximum value is calculated from the average value plus three times the standard deviation. Element values that are less or more than the cutoff limit value will be discarded. Relative frequencies are calculated for each bin and used as a feature. Relative frequency is the number of items in each bin divided by the number of items in the set. The relative frequencies of a histogram are combined and used as feature vectors. For example, B_i is the bin frequency vector of the i_{th}-histogram. The feature vector F is defined as $s_i = \left\{B_1 \| B_2 \| ... \| B_j\right\}$, where j is the number of histograms.

The new feature vectors are then sorted and selected based on a certain number of n. The purpose of feature selection is to reduce the number of features and increase accuracy [10]. There are many methods for selecting the features, such as giving scores for each feature through estimating the Bayes error rate based on kernel density estimation [11]. In this research, we use AUC score for sorting and selecting the features. The difficulty level when selecting features will increase if the features are heterogeneous [12]. This time, we do not include this factor in the discussion.

This study used a signature template for each user created during the registration process, as demonstrated in [1]. Ten original signatures were taken from each user, and the determined features were counted from these ten samples. Next, the variance of each feature component is calculated and used to quantify each feature component resulted in a quantization vector of the step Q^u size. A pair (Q^u, F&&) is regarded as a step size of a quantization vector. The quantization vector of Q^u step size is used to calculate each signature feature vector from the registration process. Then, the average value of the quantified feature vector is used as a template F&&. The feature vector templates are used to verify a signature. The quantified vectors and templates are saved. Therefore, each user will produce two files: *quantizationstep_user.txt* and *template_user.txt*.

Each signature template has a minimum and maximum thresholds. The minimum threshold is calculated from the average distance between the training data and the template minus ten times the standard deviation. If the result is less than zero, then the minimum threshold value is zero. The maximum threshold is calculated from the average distance between the training data and the template with the addition of ten times the standard deviation. Then the next step is to make a list of 50 pieces of thresholds, which are the values of the range equidistance from the minimum threshold to the maximum threshold. Each threshold is used to calculate a confusion matrix.

When signature verification is performed, the test signature (the original, skilled forgery, or random forgery signature) will be represented by the set of histogram features. By using a quantization vector of the size of the Q^u step, a quantized feature vector will be generated from the test signature. And then, calculate the quantized vector distance using the saved vector template ($\hat{P}^{u}$). The distance is calculated using the Manhattan distance. The signature will be considered genuine if the distance between the two vectors is less than the threshold and will be rejected or considered wrong if the value is greater than the threshold.

3. Result and Discussion

In this chapter, we will present and discuss the results. We used 16 types of histograms taken from Sae-Bae and Menon [1]. The proposed new features can be seen in Table 1. We used two new histograms to produce new features. The X and the Y values are obtained directly from the *x* and *y* positions when the signature is made. New features derived from histogram X are x_1, x_2, x_3, x_4, ..., x_8. Where feature x_1 is the relative frequency of bin_1 of histogram X, so is x_2-x_8, while the new features derived from the Y histogram are y_1, y_2, y_3, y_4, ..., y_8.

Table 1. The Proposed New histogram features

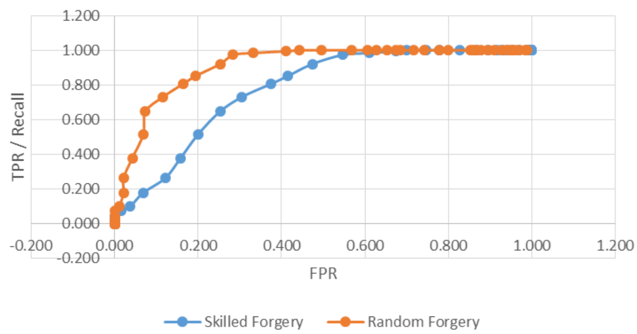
No	Histogram	Bins	Min~Max
1	X	8	(μ-3σ ~ μ+3σ)
2	Y	8	(μ-3σ ~ μ+3σ)

Table 2. Confusion Matrix using New Features

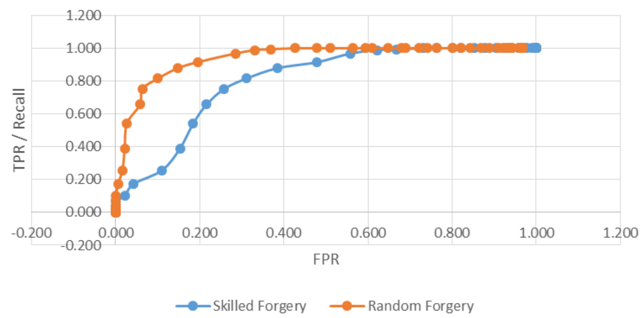
Thr	TP	FN	TN-SF	FP-SF	TN-RF	FP-RF
1	0	190	190	0	190	0
2	0	190	190	0	190	0
3	0	190	190	0	190	0
4	0	190	190	0	190	0
5	0	190	190	0	190	0
6	0	190	190	0	190	0
7	0	190	190	0	190	0
8	0	190	190	0	190	0
9	4	186	190	0	190	0
10	8	182	190	0	190	0
11	14	176	190	0	190	0
12	19	171	186	4	190	0
13	33	157	182	8	189	1
14	49	141	169	21	187	3
15	74	116	161	29	186	4
16	103	87	155	35	185	5
17	125	65	149	41	179	11
18	143	47	141	49	178	12
19	155	35	131	59	171	19
20	167	23	117	73	162	28
21	174	16	99	91	153	37
22	184	6	84	106	136	54
23	188	2	72	118	127	63
24	189	1	63	127	120	70
25	190	0	51	139	109	81

After performing feature extraction with the proposed features, the next step is to test the system and compare the confusion matrix for the original feature dataset and the dataset with new features. Table 2 shows a confusion matrix of the verification system using the histogram feature with the new features for 25 thresholds. Based on the confusion matrixes, we generate a curve with FPR on the x-axis and TPR on the y-axis at the 25 thresholds called the ROC curve (Fig. 3.a).

We used the trapezoidal method to calculate the AUC value resulting in an SF score of 0.78 and an RF score of 0.90. The RF's AUC value is greater than the SF's AUC value indicating our technique produces higher performance in handling RF cases.



(a) Without new features gave AUC SF=0.78 and RF=0.90



(b) With new features AUC SF=0.8 and RF=0.91

Figure 3. ROC curve of verification system

The ROC curve is plotted using the same method with FPR and TPR values at 25 thresholds (Figure 3.b). The experiment result shows the AUC value for SF value is 0.80, while the AUC value for RF is 0.91. To examine the robustness of our technique, we conducted experiments using *n* ranked first features. The AUC-SF and AUC-RF values in each experiment were recorded as performance indicators. This method aims to find which feature set determines the best performance. The list of feature ratings based on AUC-SF is sorted by AUC-SF score in descending order can be seen in Table 3.

Based on the features in Table 3, we carried out several experiments using datasets of the first *n* features. The dataset were formed from the first *n* new features, with *n* equal to 4, 8, 12, 13, 14, and 15. The result can be seen in Table 4.

The experiment results indicate that using new features is better than the performance without using the new features. The X and Y values of a histogram from a signature preserve important information about the signature, and the distribution of the X and Y features contributes to differentiating a signature from the others.

Table 3. Sorted features by AUC-SF score

No	Features	AUC-SF
1	x6	0.783006
2	x5	0.782202
3	x3	0.780997
4	x4	0.780402
5	y5	0.779391
	y4	0.779100
7	x7	0.778504
8	y7	0.778504
9	y6	0.777202
10	y8	0.777008
11	x2	0.776759
12	y2	0.774737
13	x1	0.774058
14	y1	0.774058
15	y3	0.773864
16	x8	0.773767

Table 4. AUC score for several datasets

No	Datasets	AUC_SF	AUC_RF
1	4 features	0.79339	0.91962
2	8 features	0.79997	0.93028
3	12 features	**0.80317**	**0.93065**
4	13 features	0.80298	0.93019
5	14 features	0.80274	0.92950
6	15 features	0.80068	0.92374
7	All features	0.79979	0.90840

A verifier can accommodate the form, velocity, and acceleration factor of a signature by utilizing the X and Y histograms as features. This method is then complemented by using 12 new features (x6, x5, x3, x4, y5, y4, x7, y7, y6, y8, x2, y2) sorted in descending order. A verifier with these steps can distinguish between original and forgery signatures better.

4. Conclusion

We developed a dynamic signature verification system using 16 new features derived from X and Y histograms. We then compared our technique to a similar technique without using the new features. The results indicated that the verification system using 16 new features gave higher AUC values for SF and RF cases. The best results are obtained when used 12 new features that produced AUC values for SF 0.80 and RF 0.93.

We plan to extend our research by taking signatures with more diverse and multiplatform devices. To manage the data, we can elaborate on other methods such as digital signal processing to extract energy from signals and used it to distinguish authentic and unauthentic signatures.

References

[1] N. Sae-Bae and N. Memon, "Online Signature Verification on Mobile Devices," *Inf. Forensics Secur. IEEE Trans. On*, vol. 9, pp. 933–947, 2014, doi: 10.1109/TIFS.2014.2316472.

[2] H. Zhang, W. Gao, X. Chen, and D. Zhao, "Learning informative features for spatial histogram-based object detection," 2005, vol. 3, pp. 1806–1811 vol. 3. doi: 10.1109/IJCNN.2005.1556154.

[3] G. Hetzel, B. Leibe, P. Levi, and B. Schiele, "3D Object Recognition from Range Images using Local Feature Histograms," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2001, vol. 2, p. II–394. doi: 10.1109/CVPR.2001.990988.

[4] Y. Serdouk, H. Nemmour, and Y. Chibani, "New Histogram-based Descriptor for Off-Line Handwritten Signature Verification," in *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*, 2018, pp. 1–5. doi: 10.1109/AICCSA.2018.8612793.

[5] Winstonnelson, Williamturin, and Trevorhastie, "STATISTICAL METHODS FOR ON-LINE SIGNATURE VERIFICATION," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 08, 2011, doi: 10.1142/S0218001494000395.

[6] M. Mshengu and M. V. Gwetu, "Online Signature Verification through Scaled Histogram of Oriented Gradients," in *2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, 2019, pp. 1–5. doi: 10.1109/ICABCD.2019.8851050.

[7] J. SWETS, "ROC Analysis Applied to the Evaluation of Medical Imaging Techniques," *Invest. Radiol.*, vol. 14, pp. 109–21, 2005, doi: 10.1097/00004424-197903000-00002.

[8] M. A. Sovierzoski, F. Mendes de Azevedo, and F. I. M. Argoud, "Performance Evaluation of an ANN FF Classifier of Raw EEG Data using ROC Analysis," in *2008 International Conference on BioMedical Engineering and Informatics*, 2008, vol. 1, pp. 332–336. doi: 10.1109/BMEI.2008.220.

[9] A. R. Rahardika and A. Tjahyanto, "Global features selection for dynamic signature verification," in *2018 International Conference on Information and Communications Technology (ICOIACT)*, 2018, pp. 348–354. doi: 10.1109/ICOIACT.2018.8350736.

[10] Y. Xue, Y. Tang, X. Xu, J. Liang, and F. Neri, "Multi-Objective Feature Selection With Missing Data in Classification," *IEEE Trans. Emerg. Top. Comput. Intell.*, pp. 1–10, 2021, doi: 10.1109/TETCI.2021.3074147.

[11] X. Xie and W. Stork, "Watermelon: a Novel Feature Selection Method Based on Bayes Error Rate Estimation and a New Interpretation of Feature Relevance and Redundancy," in *2020 25th International Conference on Pattern Recognition (ICPR)*, 2021, pp. 1360–1367. doi: 10.1109/ICPR48806.2021.9413262.

[12] H. Sulistiani and A. Tjahyanto, "Heterogeneous feature selection for classification of customer loyalty fast moving consumer goods (Case study: Instant noodle)," vol. 94, pp. 77–83, 2016.