E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 03, Nomor 01, Juni 2018 : 76 - 83

PERANCANGAN APLIKASI ANDROID IDENTIFIKASI TANDA TANGAN MENGGUNAKAN MULTI LAYER PERCEPTRON

Gagas Novandra[1)], Muhammad Zidny Naf'an[2)], Tri Ginanjar Laksana[3)]
[1, 2,3)]Institut Teknologi Telkom Purwokerto
Jl.D.I. Panjaitan No.128, Purwokerto Kidul, Purwokerto Sel., Purwokerto, Jawa Tengah 53147
e-mail: novandragagas@gmail.com [1)], zidny@ittelkom-pwt.ac.id [2)], anjarlaksana@ittelkom-pwt.ac.id [3)]

ABSTRAK

Sering terjadinya suatu kasus pemalsuan tanda tangan disebabkan karena metode yang digunakan untuk mengidentifikasi tanda tangan masih kurang baik dan tidak akurat. Hal ini dikarenakan identifikasi tanda tangan kebanyakan masih dilakukan dengan cara melihat langsung tanda tangan, beserta nama pemilik tanda tangan yang tercantum di bagian bawah tanda tangan pada sebuah dokumen. Mengidentifikasi tanda tangan dengan cara manual tentu memiliki banyak kelemahan seperti ketelitian dan ketepatan saat identifikasi yang kurang absah, sehingga pemalsuan tanda tangan sangat mungkin terjadi. Penelitian ini menggunakan metode Artificial Neural Network yang akan diterapkan pada aplikasi identifikasi tanda tangan. Neural Network merupakan metode yang dapat mendeteksi pola rumit dan tidak mengikuti seragkaian instruksi yang diberikan peneliti. Namun metode ini mampu belajar dengan sendirinya saat menghadapi permasalahan. Metode ini memiliki kelebihan yaitu kemampuan untuk memodelkan fungsi linear, komputasi paralel, dan mempunyai sifat mentolerir kesalahan (fault tolerance). Penelitian ini diharapkan dapat membantu suatu lembaga, baik itu lembaga pemerintahan maupun lembaga swasta dalam mengidentifikasi pemilik dari suatu tanda tangan yang ada pada dokumen-dokumen penting seperti dokumen pencairan dana dan dokumen surat-menyurat. Sehingga kasus pemalsuan tanda tangan dapat diminimalisir. Selain hal tersebut dalam penelitian ini juga diharapkan agar nantinya sistem identifikasi tanda tangan dapat diterapkan pada suatu lembaga atau instansi.

***Kata Kunci**: Tanda Tangan, Artificial Neural Network, Identifikasi.*

ABSTRACT

Often the occurrence of a signature forgery case is caused because the method used to identify the signature is still poor and inaccurate. This is because most signature identification is still done by looking directly at the signature, along with the name of the signature owner listed at the bottom of the signature on a document. Identifying signatures manually certainly has many weaknesses like precision and accuracy when identification is less valid, so signature falsification is possible. This research uses Artificial Neural Network method that will be applied to signature identification application. Neural Network is a method that can detect complicated patterns and does not follow the instructions given by the researchers. However, this method can learn by itself when faced with problems. This method has advantages such as the ability to model linear functions, parallel computing, and have a fault tolerance.This research is expected to help an institution, whether government agency or private institution in identifying the owner of a signature contained in important documents such as fund fluid documents and correspondence documents. So the case of signature forgery can be minimized. In addition to those mentioned in this study, it is also expected that the signature identification system can be applied to an institution or agency.

***Keywords**: Signature, Artificial Neural Network, Identification.*

I. PENDAHULUAN

Tanda tangan merupakan coretan tangan dari setiap orang yang memiliki pola tertentu dan dijadikan sebagai salah satu alat identifikasi biometrik. Identifikasi biometrik bermanfaat untuk berbagai keperluan, seperti sistem keamanan pada perangkat digital dan pelacakan identitas seseorang [1]. Tanda tangan banyak digunakan pada berbagai macam dokumen kegiatan yang memerlukan tanda tangan sebagai identifikasi dan kebenaran dari dokumen. Salah satu contoh kegiatan yang paling sering membutuhkan tanda tangan pada dokumen adalah kegiatan administrasi.

Sistem pengenalan biometrik biasanya dikembangkan untuk dua tujuan utama, yaitu identifikasi dan verifikasi. Sistem biometrik dapat dimodelkan berdasarkan sifat fisik dan sifat perilaku. Sifat fisik seperti wajah, sidik jari, dan iris sangat unik untuk setiap individu. Sementara sifat perilaku seperti suara, gaya berjalan dan tanda tangan [2]. Identifikasi pola tanda tangan sangatlah penting dilakukakan untuk mengidentifikasi pemilik sebenarnya dari suatu tanda tangan. Berdasarkan hasil studi literatur, didapatkan kasus – kasus pemalsuan tanda tangan:

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 03, Nomor 01, Juni 2018 : 76 - 83

Tabel 1.1 Kasus Pemalsuan Tanda Tangan

Sumber	Tahun	Kasus
Merdeka.com	2013	Pemalsuan tanda tangan dilakukan oleh dua orang dengan memalsukan tanda tangan seorang Gubernur Maluku Utara. Pemalsuan dilakukan guna mengambil alih suatu lahan pertambangan milik sebuah perusahaan perkebunan di Maluku Utara.
NEWS Republika.co.id	2014	Seorang suami memalsukan tanda tangan istrinya sendiri pada surat persetujuan dan kuasa tanah. Surat tersebut digunakan untuk menjual tanah karena sang suami memiliki hutang di suatu bank.
Detiknews	2015	Kasus pemalsuan tanda tangan dialami oleh salah satu artis Indonesia. Seseorang memalsukan tanda tanga artis tersebut pada dokumen proposal program siaran ke salah satu stasiun TV nasional.
Kantor Berita Politik RMOL.co	2016	Mantan sekretaris kabinet suatu lembaga swadaya masyarakat (LSM) di Indonesia memalsukan tanda tangan presiden dari LSM tersebut untuk mengubah akte notaris milik LSM.
Timlo.net	2016	Pemalsuan tanda tangan dilakukan oleh mantan manager suatu club sepakbola Indonesia, dengan memalsukan tanda tangan temannya untuk penarikan uang di salah satu Bank Kota Solo.
Kompas.com	2017	Seorang istri memalsukan tanda tangan suaminya pada surat kuasa yang seolah-olah diberikan kepadanya untuk mengambil surat tanda registrasi di suatu Kantor Pos Surabaya.
Detiknews	2017	Kasus tentang pemalsuan tanda tangan yang belum lama ini terjadi dilakukan oleh seorang mahasiswa dari salah satu universitas ternama. Mahasiswa tersebut memalsukan tanda tangan dengan tujuan untuk mendapatkan beasiswa S2 di universitas ternama lain.

Berdasarkan Tabel 1.1 diatas dapat dikemukakan bahwa kasus pemalsuan tanda tangan dapat terjadi, antara lain disebabkan oleh identifikasi yang kurang baik. Identifikasi tanda tangan kebanyakan dilakukan dengan cara manual, yaitu dengan membandingkan secara langsung tanda tangan beserta nama pemilik tanda tangan yang biasanya tercantum di bagian bawah tanda tangan pada sebuah dokumen. Mengidentifikasi tanda tangan dengan cara manual tentu memiliki banyak kelemahan. Sehingga ketelitian dan ketepatan hasil yang diinginkan seringkali kurang memuaskan [3].

Penelitian ini akan berfokus pada pendekatan *offline*, karena kasus pemalsuan tanda tangan seringnya terjadi pada dokumen-dokumen yang memerlukan tanda tangan secara manual pada kertas. Beberapa penelitian yang dilakukan dengan berdasarkan pendekatan secara *offline*, yaitu oleh Bansal, dkk [4] yang menggunakan metode *Graph Matching* pada sistem verifikasi citra tanda tangan dan menggunakan metode *Hungarian* untuk menemukan kesamaan geometri, menunjukkan tingkat akurasi sistem lebih dari 89%.

Penelitian lain pada sistem verifikasi tanda tangan dilakukan olehBhatia [5]yang munggunakan metode *ArtificialNeural Network*dengan model *Feed Forward Backpropagation Neural Network*untuk klasifikasi tanda tangannya dan *Levenberg-Marquardt* (LM) sebagai algoritma training datanya.Dari hasil penelitian, tingkat akurasi dari aplikasi secara umum mencapai 98,66%.

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 03, Nomor 01, Juni 2018 : 76 - 83

II. METODE

A. *Artificial Neural Network*

Artificial Neural Network atau jaringan syaraf tiruanmerupakan sistem pemroses informasi yang mempunyai karakteristik kinerja khusus yang sama seperti jaringan syaraf biologis. Jaringan syaraf tiruan telah dikembangkan secara umum sebagai model matematika dari sifat kognitif manusia atau syaraf biologi, dengan asumsi bahwa [6]:

1. Pemrosesan informasi terjadi pada banyak elemen sedehana yang disebut *neuron*.
2. Sinyal lewat diantara banyak *neuron* melalui koneksi.
3. Setiap koneksi mempunyai bobot yang bersesuaian, yang mana dalam kebanyakan jaringan syaraf banyak sinyal yang ditransmisikan.
4. Setiap *neuron* menerapkan fungsi aktivasi (biasanya non linear) ke jaringan inputnya (jumlah dari bobot sinyal input) untuk menentukan sinyal output.

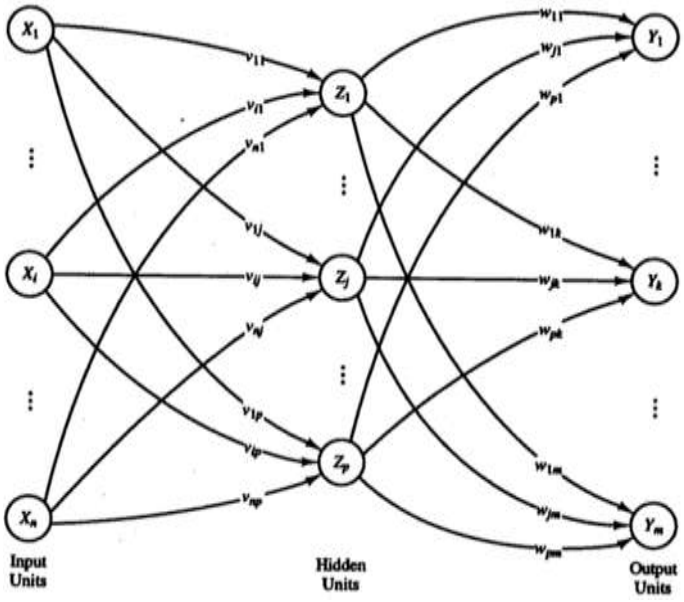
Sebuah jaringan syaraf dikelompokkan berdasarkan:

1. Pola dari koneksi antara banyak neuron (arsitektur).
2. Metode untuk menentukan bobot pada koneksi (algoritma pelatihan atau pembelajaran pola).
3. Fungsi aktivasi.

Dalam *ArtificialNeuralNetwork*, kerangka *neuron* disusun dalam *layer-layer* yang membentuk suatu pola koneksi. Kerangka ini disebut *netarchitecture* (arsitektur jaringan).

B. *Multilayer Perceptron*

Multilayer Perceptron (MLP) merupakan model jaringan *perceptron* yang menggunakan kerangka jaringan *multilayer* pada arsitekturnya.*Perceptron*merupakan salah satu model dari jaringan syaraf tiruan. Pada *multilayer network*, memiliki satu atau lebih *layer* tambahan yang menghubungkan antara unit *input* dan unit *output*. *Layer* ini disebut *hidden units* (unit tersembunyi). Secara umum, terdapat layer bobot antara tiap *layer* unit yang berdekatan (*input*, *hidden* atau *output*).



Gambar 1. *Multilayer Network*

MLP adalah *classifier* linier yang menggunakan teknik *supervisedlearning*, untuk mengubah himpunan *input* menjadi himpunan *output*. Klasifikasi ini didasarkan pada fungsi prediktor linier, yang menggabungkan satu *set* bobot dengan vektor masukan. Berikut formula dari MLP [7]:

$$Y = F(x) = \varphi\left(\sum_{j=1}^{n} W_j X_j + b\right) = \varphi(W^T X + b)$$

Keterangan:
$Y = F(x)$ = *output* yang dihasilkan

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 03, Nomor 01, Juni 2018 : 76 - 83

W = bobot vektor
X = *input* vektor
b = bias
φ = fungsi aktivasi

III. HASIL DAN PEMBAHASAN

Tahapan-tahapan penelitian yang akan dilakukan diantaranya:

A. Pemisahan *Dataset* menjadi Data *Training* dan Data *Testing*

Dataset akan dipisahkan menjadi data *training* dan data *testing* dengan menggunakan algoritma K-*foldcross validation*. Data *training* dibagi menjadi k buah *subset* (sub-himpunan), dimana k adalah nilai dari *fold*. Misal jika nilai dari k yaitu 5 dengan jumlah *dataset* yang digunakan 900 tanda tangan asli, maka skema pembagian *dataset* menjadi data *training* dan *testing* sebagai berikut:

Tabel 3.1 Skema Algoritma K-*Fold Cross Validation*

180 *Dataset* (126 Data *Training*, 54 Data *Testing*)	180 *Dataset* (126 Data *Training*, 54 Data *Testing*)	180 *Dataset* (126 Data *Training*, 54 Data *Testing*)	180 *Dataset* (126 Data *Training*, 54 Data *Testing*)	180 *Dataset* (126 Data *Training*, 54 Data *Testing*)

Rasio perbandingan data *training* dan data *testing* yang akan digunakan yaitu 70:30. Hal ini dikarenakan data tanda tangan yang digunakan cukup banyak, sehingga dibutuhkan proses training yang lebih lama agar tingkat akurasi yang dihasilkan besar.

B. Pra-Pemrosesan

Pada tahap ini, citra RGB pada data *training* dan data *testing* dikonversi menjadi citra *grayscale*. Setelah menjadi citra *grayscale*, dilakukan proses segmentasi untuk memisahkan objek citra dari *background* citra. Citra hasil segmentasi ini merupakan citra biner. Segmentasi citra dilakukan dengan menggunakan metode pengambangan. Setelah citra biner didapatkan, *resize* citra dilakukan untuk membuat resolusi dan ukuran pada setiap citra sama.

C. Ekstraksi Fitur

Setelah citra biner didapatkan, langkah selanjutnya yaitu dilakukan ekstraksi fitur pada data *training* dan data *testing* dengan menggunakan metode *Discrete Cosine Transform* (DCT).DCT mengubah sinyal masukan domain spasial di masing-masing sel citra tanda tangan menjadi domain frekuensi dalam bentuk koefisien DCT[8]. Hasil dari ekstraksi fitur berupa ciri atau nilai dari setiap citra tanda tangan berdasarkan parameter yang digunakan.Berikut merupakan formula yang digunakan untuk mendapatkan koefisien DCT dari sel citra (f (x, y)):

$$G(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y).cos\left(\frac{(2x+1)u\pi}{2M}\right).cos\left(\frac{(2y+1)v\pi}{2N}\right)$$

Untuk

$$\alpha(u) = \begin{cases} 1/\sqrt{M}, & u = 0 \\ \sqrt{2/M}, & 1 \le u \le M-1 \end{cases}$$

$$\alpha(v) = \begin{cases} 1/\sqrt{N}, & v = 0 \\ \sqrt{2/N}, & 1 \le v \le N-1 \end{cases}$$

Keterangan:
$f(x, y)$ = x, y merupakan elemen citra yang direpresentasikan oleh matriks f
M, N = ukuran blok citra yang sudah dilakukan DCT
u, v = persamaan menghitung satu entri gambar yang berubah dari nilai nilai piksel matriks citra asli

D. Training

Pada tahap ini, setiap data *training* dilatih untuk mendapatkan nilai bobot dari setiap tanda tangan. Proses *training* ini dapat dilakukan secara berulang, hingga didapatkan nilai bobot yang optimal. Nilai bobot optimal inilah yang akan digunakan dalam aplikasi *android* sebagai identitas dari setiap tanda tangan.

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 03, Nomor 01, Juni 2018 : 76 - 83

E. Perancangan Aplikasi Identifikasi Tanda Tangan

Aplikasi identifikasi tanda tangan akan dibuat dengan menggunakan bahasa pemrograman *Java* pada aplikasi Android Studio. Pada aplikasi, pengguna dibedakan menjadi 2 yaitu *user* dan dan *admin*.

Gambar 2. Tampilan Awal Aplikasi

User hanya berperan sebagai pemakai saja. Ketika pengguna aplikasi masuk sebagai *user*, aplikasi akan melanjutkan pada proses pengambilan citra tanda tangan. Proses pengambilan citra dapat diawali dengan menggunakan kamera sebelum memilih citra yang sudah tersimpan di dalam *gallery*.

Gambar 3. Tampilan Ambil Citra

Ketika citra sudah dipilih dari *gallery*, sistem akan mengalihkan ke proses identifikasi. Dalam proses ini, terdapat dua tombol cek hasil dan *gallery*. Tombol cek hasil digunakan untuk mengidentifikasi citra tanda tangan yang sudah dipilih sebelumnya. Pada kolom pemilik dan parameter akan muncul ketika proses identifikasi selesai. Tombol *gallery* digunakan jika ingin mengganti citra tanda tangan yang ingin diidentifikasi.

Gambar 4. Tampilan Identifikasi Kepemilikan

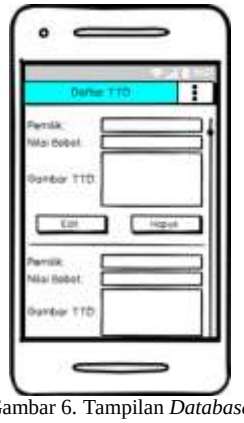
Selain *user*, pengguna dalam aplikasi ini yaitu *admin*. *Admin* berperan sebagai pengelola *database* citra tanda tangan. Sebelum pengguna masuk sebagai seorang *admin*, proses verifikasi harus dilakukan terlebih dahulu. Pengguna harus mengisikan *username* dan *password* milik *admin*.

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 03, Nomor 01, Juni 2018 : 76 - 83

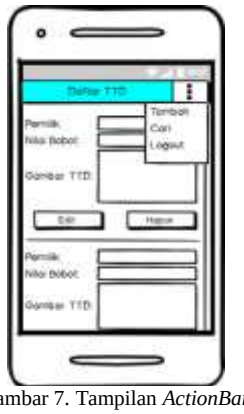
Gambar 5. Tampilan *LoginAdmin*

Setelah proses verifikasi selesai, sistem akan mengalihkan *admin* ke *database*. Dalam *database*, informasi dari setiap citra berupa pemilik tanda tangan, nilai bobot tanda tangan, dan citra tanda tangan.



Gambar 6. Tampilan *Database*

Dalam setiap kolom inforamsi citra, terdapat dua tombol fungsi yaitu *edit* dan hapus. *Edit* digunakan untuk merubah informasi dari citra. Sedangkan hapus digunakan untuk informasi suatu citra dari *database*. Dalam *database*, terdapat juga fungsi lain yaitu tambah data, cari data dan *logout*. Fungsi ini ada dalam tombol *actionbar*.

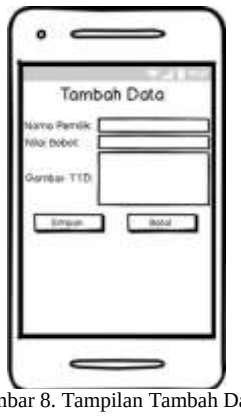


Gambar 7. Tampilan *ActionBar*

Fungsi tambah digunakan untuk menambah data berupa citra tanda tangan beserta informasi yang dibutuhkan. Dalam menu tambah data, terdapat dua tombol fungsi yaitu simpan dan batal. Tombol simpan untuk menyimpan informasi citra ke dalam *database*. Tombol batal digunakan jika proses tambah data tidak jadi dilakukan. Sedangkan fungsi *logout* untuk mengeluarkan pengguna sebagai *admin*.

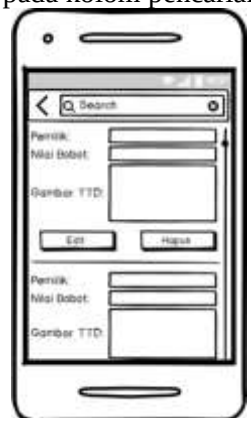
E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 03, Nomor 01, Juni 2018 : 76 - 83



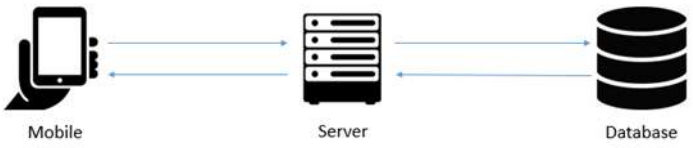
Gambar 8. Tampilan Tambah Data

Fungsi cari digunakan untuk mencari suatu citra dalam *database*. Fungsi ini berguna jika data dalam *database* banyak dan membutuhkan waktu lama jika dicari dengan men-*scroll* kebawah. Proses pencarian dapat dilakukan dengan menuliskan nama pemilik tanda tangan pada kolom pencarian.



Gambar 9. Tampilan Pencarian Data

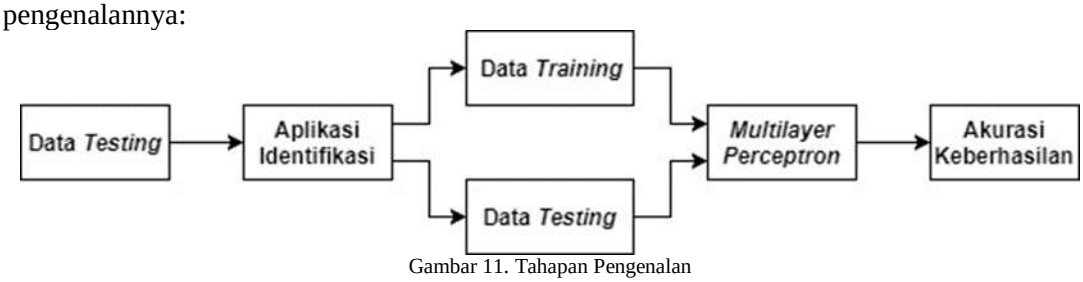
Untuk lebih menjelaskan alur sistem dalam melakukan proses identifikasi tanda tangan, berikut merupakan arsitektur dari sistem yang akan dibuat:



Gambar 10. Arsitektur Sistem

F. Pengenalan

Proses pengenalan dilakukan dengan menggunakan aplikasi identifikasi tanda tangan berbasis *Android*. Algoritma pengenalan menggunakan model *Artificial Neural Network*: *Multi Layer Perceptron*. Berikut merupakan alur proses pengenalannya:



Gambar 11. Tahapan Pengenalan

Untuk skenario pengujian akurasi dari algoritma *Multi Layer Perceptron*, dapat dilihat seperti tabel berikut:

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 03, Nomor 01, Juni 2018 : 76 - 83

IV. KESIMPULAN

Berdasarkan penelitian yang sudah dilakukan maka didapatkan kesimpulan sebagai berikut:

1. Dengan menggunakan rasio perbandingan 70:30 pada data *training* dan data *testing* dapat meningkatkan tingkat akurasi metode *Multilayer Perceptron* dalam proses identifikasi tanda tangan.
2. Aplikasi dapat mengetahui pemilik dari setiap citra tanda tangan, sehingga mengurangi kemungkinan pemalsuan tanda tangan.

DAFTAR PUSTAKA

[1] T. Handhayani, A. R. Yohannis, and L. Hiryanto, "Pengembangan Aplikasi Identifikasi Biometrik Bebrbasis Perangkat Mobile untuk Alternatif Sistem Keamanan Digital," 2016.

[2] V. Iranmanesh *et al.*, "Online handwritten signature verification using neural network classifier based on principal component analysis.," *ScientificWorldJournal.*, vol. 2014, p. 381469, 2014.

[3] A. A. K. O. Sudana, "Sistem verifikasi citra tandatangan dengan metode pola busur terlokalisasi," *Maj. Ilm. Teknol. Elektro*, vol. 5, no. 2, 2006.

[4] A. Bansal, B. Gupta, G. Khandelwal, and S. Chakraverty, "Offline Signature Verification Using Critical Region Matching," *Int. J. Signal Process. Image Process. Pattern*, vol. 2, no. 1, pp. 57–70, 2009.

[5] M. Bhatia, "Off-Line Hand Written Signature Verification," *Int. J. Appl. or Innov. Eng. Manag.*, vol. 2, no. 5, pp. 108–116, 2013.

[6] L. Fausett, *Fundamentals of Neural Networks*, no. 1. Prentice-Hall, 1994.

[7] A. S. Shah, M. Shah, M. Fayaz, and F. Wahid, "Forensic Analysis of Offline Signatures Using Multilayer Perceptron and Random Forest," *Int. J. Database Theory Appl.*, vol. 10, no. 1, pp. 139–148, 2017.

[8] K. S. Khabiya, S. S. Sonawane, L. V Sonawane, and T. S. Sali, "Online Signature Verification System using DRT , DCT and K-NN Classifier," *IJIRST -International J. Innov. Res. Sci. Technol.*, vol. 3, no. 1, pp. 22–27, 2016.