p-ISSN 2301–4156 | e-ISSN 2460–5719

Model Berbasis CNN untuk Estimasi dan Autentikasi *Copy Detection Pattern*

Syukron Abu Ishaq Alfarozi[1], Azkario Rizky Pratama[2]

[1,2] Departemen Teknik Elektro dan Teknologi Informasi, Fakultas Teknik Universitas Gadjah Mada, Yogyakarta 55281 INDONESIA (tel.: 0274-5555; fax: 0274-4321; email: [1]syukron.abu@ugm.ac.id, [2]azkario@ugm.ac.id)

[Diterima: 29 November 2022, Revisi: 24 Januari 2023]
Corresponding Author: Syukron Abu Ishaq Alfarozi

INTISARI — Pemalsuan merupakan salah satu tindak kriminal di abad ke-21. Salah satu metode untuk mengatasi pemalsuan produk adalah *copy detection pattern* (CDP) yang ditempelkan pada produk. CDP merupakan sebuah pola peka salinan yang menyebabkan penurunan kualitas pola setelah proses cetak dan pindai. Jumlah informasi yang hilang digunakan untuk membedakan CDP asli dan palsu. Makalah ini mengusulkan model estimasi CDP berdasarkan *convolutional neural network* (CNN), yang disebut CDP-CNN. CDP-CNN mengatasi ketergantungan spasial dari *patch* citra. Dengan demikian, CDP-CNN mestinya lebih baik daripada model yang menggunakan arsitektur *multi layer perceptron* (MLP). Model yang diusulkan menghasilkan estimasi *bit error rate* (BER) sebesar 9,91% pada metode estimasi *batch*. BER ini 9% lebih rendah daripada BER metode sebelumnya yang menggunakan model MLP *autoencoder*. Model yang diusulkan mempunyai jumlah parameter yang lebih sedikit dibandingkan metode sebelumnya. Pengaruh *preprocessing*, penggunaan *unsharp mask*, diuji menggunakan metode pengujian statistik. Pengaruh *preprocessing* tidak memiliki perbedaan yang signifikan kecuali dalam skema estimasi *batch*, yaitu filter *unsharp mask* mengurangi BER sebesar paling tidak 0,5%. Selain itu, model yang diusulkan ini juga digunakan untuk metode autentikasi. Autentikasi menggunakan model estimasi ini memiliki pemisahan distribusi yang baik untuk membedakan CDP palsu dan asli. Maka, CDP masih dapat digunakan sebagai metode autentikasi dengan kinerja yang reliabel. CDP membantu anti-pemalsuan pada distribusi produk dan mengurangi akibat negatif pada berbagai sektor ekonomi.

KATA KUNCI — *Copy Detection Pattern*, *Convolutional Neural Network*, Anti-Pemalsuan.

I. PENDAHULUAN

Pemalsuan adalah sebuah pelanggaran terhadap pemilik kekayaan intelektual dan merupakan sebuah tindak kriminal yang menimbulkan dampak negatif bagi berbagai sektor ekonomi, hingga banyak yang menyebutkan bahwa pemalsuan adalah tindak kriminal abad ke-21 [1], [2]. *Organization for Economic Cooperation and Development* (OECD) dan EUIPO menerbitkan laporan bersama pada tahun 2019 tentang tren perdaganan barang palsu dan bajakan berdasarkan data penyitaan dunia tahun 2016 [1], [3]. Laporan tersebut menemukan bahwa perdagangan barang palsu dan bajakan mencapai jumlah $509 miliar (3,3% dari total perdagangan dunia). Jumlah ini meningkat dari tahun 2013, menjadi $461 miliar (2,6% dari total perdagangan dunia). Jumlah tersebut meningkat walaupun keseluruhan perdagangan dunia relatif melambat. Terlebih lagi, jumlah tersebut hanya merepresentasikan produk yang disita dan tidak mewakili sepenuhnya dampak pemalsuan pada semua sektor ekonomi, termasuk produsen barang asli, pelanggan, dan pemerintah.

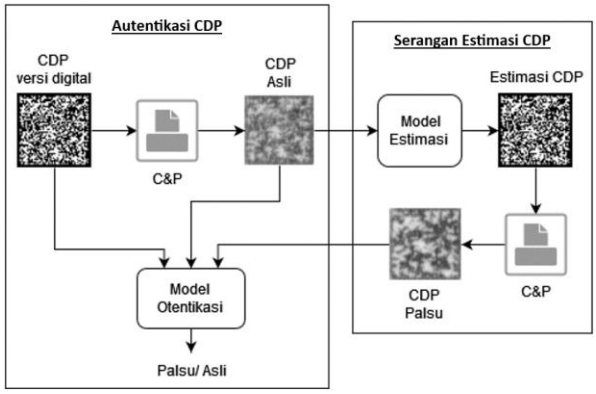
Barang-barang yang dipalsukan berpengaruh langsung terhadap penjualan produk asli. Perusahan-perusahaan di seluruh dunia mengalami kerugian miliaran dolar AS setiap tahun akibat pemalsuan barang. Menurut sekretaris jenderal International Chamber of Commerce (ICC), pabrik-pabrik multinasional kehilangan sekitar 10% pendapatan *top-line*-nya akibat pemalsuan [1].

Usaha menghadapi pemalsu barang menmbutuhkan keterlibatan dan komitmen semua pihak yang terkait. Mike O'Neil, Sekretaris ISO/TC 247 tentang penanggulangan dan pengendalian penipuan menyatakan bahwa perang melawan pemalsuan dilakukan pada empat area utama: 1) tindakan legislatif untuk melindungi kekayaan intelektual dan menghukum pemalsuan; 2) badan bea cukai nasional untuk mencegah masuknya barang palsu ke suatu negara, 3) usaha industri swasta untuk menciptakan teknologi anti-pemalsuan; dan 4) pengembangan standar nasional dan internasional [1].

Sebagai pihak yang terkena dampak paling besar, produsen barang asli perlu mengembangkan pendekatan untuk melindungi keaslian produknya. Berbagai teknologi telah diimplementasikan untuk mencapai perlindungan produk yang aman. Masing-masing dibedakan berdasarkan biaya, kecanggihan, dan efektivitasnya dalam mendeteksi pemalsuan produk. Teknologi yang sering diterapkan meliputi hologram, kartu cerdas, penanda dan tinta biometrik, serta *copy detection pattern* (CDP) [4].

CDP merupakan salah satu solusi yang dikembangkan untuk mengatasi pemalsuan. CDP adalah sebuah citra digital yang *copy-sensitive* dengan properti spesifik yang akan dicetak dan ditempelkan pada produk. CDP mendeteksi produk asli dan produk palsu berdasarkan prinsip kehilangan informasi [5]. Dalam setiap proses cetak-dan-pindai (C&P) sebuah citra digital, beberapa informasi akan hilang akibat degradasi citra dan derau akan tertambahkan karena proses pencetakan. Maka, tiap kali sebuah citra dicetak atau diproses, akan ada perubahan struktural dan kualitas pada citra yang dihasilkan. Proses ini yang akan membedakan cetakan pertama CDP, yang ditemukan pada produk asli dari CDP pada produk palsu. C&P merupakan proses stokastik dengan distribusi probabilitas acak yang dapat dianalisis secara statistis, tetapi sulit diprediksi. CDP menghasilkan sebuah citra dengan konten tidak dapat diprediksi untuk mencegah pemalsu untuk mengetahui karakteristik eksplisit dan implisit dari sebuah citra. Citra-citra yang menyimpan informasi maksimum seperti citra-mirip-derau merupakan citra yang paling sulit ditiru. Hal ini dapat dicapai dengan menetapkan sebuah nilai yang benar-benar acak dan tidak dapat diprediksi pada tiap piksel. Maka, dapat disimpulkan bahwa citra yang paling sulit ditiru adalah citra

p-ISSN 2301–4156 | e-ISSN 2460–5719



Gambar 1. Alur kerja autentikasi dan estimasi CDP.

yang tersusun dari derau murni, yang memiliki entropi maksimum. Untuk keperluan replikasi, pembuatan pola dapat menggunakan kunci rahasia atau kata sandi sebagai salah satu masukan dari fungsi *hash*.

Seseorang dapat menyalin CDP asli melalui proses C&P dan mengestimasi pola aslinya, yaitu templat atau CDP versi digitalnya. Hasil estimasi yang dicetak kedua kalinya disebut CDP palsu. Proses ini disebut serangan estimasi, seperti yang ditunjukkan pada Gambar 1. Mengestimasi pola CDP merupakan salah satu hal penting dalam restorasi citra CDP. Jika hasil restorasi memberikan *bit error rate* (BER) yang rendah, seseorang akan dapat membuat CPD palsu yang sulit dibedakan dari aslinya [6]. Autentikasi adalah sebuah proses untuk membedakan CDP asli dan CDP palsu. Model autentikasi dapat berupa *machine learning* atau model statistik. Proses autentikasi dan estimasi diperlihatkan pada Gambar 1.

Deep learning (DL) telah menjadi sebuah teknologi baru yang dapat diaplikasikan pada beberapa bidang [7]–[9]. Ada beberapa manfaat DL untuk memprediksi pola tersembunyi dan memulihkan isyarat tertentu dengan menghilangkan derau [10]–[12]. Penelitian ini berfokus untuk meningkatkan metode estimasi dan autentikasi CDP yang telah diteliti sebelumnya [13]. Menurunkan galat (*error*) prediksi pada estimasi CDP meningkatkan *false positive* pada autentikasi CDP. Hal ini menunjukkan efektivitas CDP, yaitu dapat disalin atau tidak. Dengan demikian, serangan estimasi CDP harus dimitigasi dengan metode autentikasi yang lebih baik untuk mendeteksi CDP asli dan palsu. Pada makalah ini, digunakan model DL, yaitu model *convolutional neural network* (CNN), untuk memprediksi pola CDP. Dibandingkan dengan penelitian sebelumnya [13], model yang diusulkan mampu mencapai kinerja yang lebih baik dalam mengestimasi pola CDP.

Selain itu, filter *unsharp mask* sebagai sebuah metode prapemrosesan masukan yang digunakan dalam [13] akan diselidiki, yaitu dapat meningkatkan kinerja model atau tidak. Proses autentikasi yang digunakan adalah sebuah skor ambang berdasarkan BER estimasi CDP dari model estimasi untuk menentukan CDP asli atau palsu. Maka, kontribusi makalah ini dapat dirangkum sebagai berikut:

- mendesain arsitektur dari model estimasi berbasis CNN,
- membandingkan pengaruh prapemrosesan citra CDP masukan untuk model CNN yang dikembangkan, dan
- mengevaluasi autentikasi CDP menggunakan model estimasi.

II. METODE CDP

Beberapa penelitian sebelumnya membahas berbagai aspek CDP. Sebuah metrik baru (fitur yang diekstraksi) diusulkan dalam [14], 486 tipe fitur, untuk digunakan sebagai nilai kuantitatif dari evaluasi keaslian CDP dengan kinerja yang lebih baik daripada metrik yang sudah biasa digunakan. Penelitian tersebut membandingkan metrik yang diusulkan terhadap metrik-metrik berikut: 1) metrik entropi, 2) metrik *Fourier domain sharpness*, 3) metrik *wavelet domain sharpness*, dan 4) metrik galat prediksi. Metrik-metrik yang ada dalam penelitian tersebut dibandingkan dan dievaluasi pada lima metode restorasi yang sudah ada sebagai bentuk serangan pada CDP: 1) penapisan Wiener, (2) penapisan *constrained least squares*, 3) algoritme Lucy-Richardson, 4) metode filter, dan (5) filter *Photoshop's smart sharpen*. Metode-metode serangan tersebut berusaha meningkatkan kualitas CDP yang dipalsukan agar tidak dapat dibedakan dari cetakan asli. Tiap tipe serangan kemudian dievaluasi dengan tiap tipe fitur dan dibandingkan berdasarkan laju galat (*error rate*) tiap pasangan. Laju galat yang lebih tinggi menandakan kinerja metode serangan yang lebih baik. Maka, hal ini menandakan keandalan yang lebih rendah dari metrik yang sedang dievaluasi.

Dari evaluasi CDP asli, kedua *wavelet* dan 486 tipe fitur yang diusulkan mendapatkan laju galat nol. Evaluasi terhadap serangan Photoshop menghasilkan kinerja terbaik pada 486 tipe fitur, yaitu mendapatkan laju galat yang lebih rendah, yaitu 2,43%. Evaluasi pada serangan *sharpness* (a = 0,5), 486 tipe fitur juga mencapai laju galat yang paling rendah, yaitu 2,47%. Demikian pula dengan serangan *sharpness* (a = 1), 486 fitur yang diusulkan mendapatkan laju galat yang paling rendah, sebesar 4,83%. Evaluasi serangan filter Wiener merupakan yang terendah pada fitur *wavelet*, dengan laju galat 1,83%, sedangkan 486 tipe fitur mendapatkan laju galat yang lebih tinggi, yaitu 2,80%. Evaluasi serangan Lucy-Richardson adalah yang terendah pada fiture *wavelet*, dengan laju galat 6,47% dan 486 tipe fitur memperoleh laju galat yang lebih rendah, yaitu 2,57%. Evaluasi serangan penapisan *constrained least squares* adalah yang terendah pada tipe fitur *wavelet* dengan erro rate sebesar 0,93% dan 486 tipe fitur mendapatkan laju galat yang lebih tinggi, yaitu 2,23%. 486 tipe fitur yang diusulkan memperoleh laju galat yang lebih rendah pada tiap metode serangan dibandingkan dengan metrik-metrik yang lain, kecuali pada dua metode serangan (filter Wiener dan penapisan *constrained least squares*).

Para peneliti juga mengusulkan sebuah *classifier* satu-kelas yang baru dengan mengadopsi *classifier* satu kelas *support vector domain description* (SVDD), yang sesuai untuk masalah kelas tidak seimbang. Kinerjanya dievaluasi dengan tiga rasio: 1) rasio *false positive* terhadap sampel positif (*false alarm* atau FR); 2) rasio *false negative* terhadap sampel negatif (*missing alarm* atau FA); dan 3) laju galat (PE). Evaluasi dilakukan dua kali, menggunakan semua 486 tipe fitur yang dibangkitkan dan hanya menggunakan 14 tipe fitur terpilih dengan laju galat yang rendah. Untuk penggunaan 486 fitur, *classifier* SVDD memperoleh FR 16,67%, FA 6,85%, dan PE 7,15%. Ketika menggunakan 14 tipe fitur, *classifier* SVDD mencapai skor kinerja FR 6,67%, FA 8,54%, dan PE 8,48%.

Referensi [15] menggunakan sebuah *one class support vector machine* (OC-SVM) untuk metode autentikasi. Penelitian ini bertujuan memeriksa kelayakan autentikasi CDP pada kondisi nyata, dengan menggunakan kode-kode yang dicetak pada *printer* industri dan difoto menggunakan ponsel. Kemampuan CDP untuk melakukan autentikasi dievaluasi terhadap empat jenis salinan palsu. Hasilnya menunjukkan bahwa kombinasi teknik *machine learning* dan kemampuan

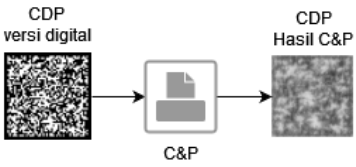
p-ISSN 2301–4156 | e-ISSN 2460–5719

tingkat lanjut ponsel modern memungkinkan dilakukannya autentikasi CDP bahkan pada salinan palsu yang tidak diketahui. Namun, digunakan ekstraksi fitur manual sebelum citra dimasukkan ke *classifier*. Kinerja *classifier* ini bergantung pada tipe fitur yang digunakan dalam penelitian.

Beberapa metode estimasi dibandingkan terhadap dua metode dasar lainnya [16]: 1) alternatif estimasi templat berdasarkan algoritme LDA dan 2) binerisasi berdasarkan *thresholding* adaptif Otsu. Metode-metode estimasi tersebut kemudian dievaluasi dengan menerapkan metrik-metrik kesamaan (*similarity*) berikut: 1) jarak Hamming untuk citra-citra biner (HAMMING); 2) *structural similarity index* (SSIM); 3) indeks Jaccard (JACCARD); dan 4) *normalized cross-correlation* (CORR). Kinerja metode estimasi diukur sepanjang jangkauan kerapatan kode (*code density*), dari nilai entropi yang lebih rendah ke yang lebih tinggi, pada sebuah *dataset* yang dibangkitkan dari dua peranti C&P yang berbeda. Pada kerapatan tertinggi yang diuji 50% dengan jarak Hamming sebagai metrik, metode estimasi yang diusulkan mencapai probabilitas galat 6,17% dan 7,57% dari masing-masing peranti C&P, lebih rendah daripada dua metode dasar, 18,13% dan 20,01% untuk metode Otsu serta 15,24% dan 16,34% pada metode LDA. Selanjutnya, metode yang diusulkan tersebut dievaluasi lebih lanjut dengan penggunaan serentak pasangan metrik agar hasil yang diharapkan menunjukkan keterpisahan antara produk asli dan palsu. Pasangan HAMMING dan SSIM menunjukkan kinerja terbaik, dengan *miss score* terendah 5,05% dan *FA score* 6,88% [16].

Dataset CDP yang terdiri atas templat digital, CDP asli, dan CDP palsu dikumpulkan dalam [13]. Penelitian ini bereksperimen dengan *dataset-dataset* yang terdiri atas 1) cetakan CDP unik (5.000 yang asli dengan templatnya dan 10.000 salinan) dan 2) cetakan CDP tiap *batch* (2.500 yang asli dengan templatnya dan 10.000 salinan). BER digunakan sebagai metrik untuk mengevaluasi efektivitas sebuah serangan estimasi. BER terkecil menunjukkan serangan estimasi yang lebih baik. Serangan estimasi "Otsu+*unsharp*" menggunakan parameter radius 2.875 dan parameter *amount* 10. Serangan estimasi dengan pendekatan *neural network* juga dilakukan. Citra-citra dibagi menjadi *patch-patch* dengan ukuran 13 × 13 = 169. Kemudian, digunakan dua arsitektur yang diusulkan: 1) *fully connected neural network* dengan 2, 3, dan 4 lapisan tersembunyi (FC2, FC3, FC4) dengan ukuran masing-masing lapisan sama dengan ukuran masukan (169); dan 2) model *bottleneck DNN* (BN DNN) dengan dua lapisan tersembunyi *fully connected* berukuran 128 dan 64 pada bagian *encoder* dan *decoder* dan representasi laten berukuran 32. Arsitektur ini diimplementasikan ulang dari penelitian sebelumnya [17]. Parameter-parameter pelatihan berupa jumlah *epoch* 25 dan ukuran *batch* 128 diimplementasikan, dengan ReLU sebagai fungsi aktivasi, *mean squared error* (MSE) sebagai *loss function*, dan Adam [18] dengan laju pembelajaran 10^{-3} sebagai pengoptimasi. Pendekatan dengan hasil terbaik (persentase BER terendah) adalah serangan estimasi menggunakan BN DNN dengan rata-rata BER 23,27% pada serangan estimasi unik dan 18,47% pada serangan estimasi *batch*. Skor korelasi Pearson digunakan sebagai metrik untuk uji keaslian antara CDP templat dan CDP yang diuji pindai.

Pada makalah ini, model yang diusulkan dan metode autentikasi dievaluasi menggunakan *dataset* dalam [13], yang telah tersedia untuk umum dan relatif baru, yaitu dipublikasikan pada tahun 2022.



Gambar 2. Proses cetak dan pindai (C&P) menyebabkan degradasi kualitas gambar dari pola CDP.

III. *COPY DETECTION PATTERN* (CDP)

CDP adalah pola biner yang sangat kecil dan rapat yang sensitif secara spasial (*spatially sensitive*) pada proses C&P [13]. Ide utama dalam CDP adalah prinsip kehilangan informasi, yaitu tiap kali citra digital dicetak dan dipindai, kualitas citra selalu berkurang. Gambar 2 mengilustrasikan prinsip kehilangan informasi selama proses C&P. Hal ini menunjukkan bahwa proses C&P pada CDP mustahil diprediksi secara sempurna karena polanya yang sangat sensitif, yaitu sangat kecil sehingga akan tergdegradasi oleh kemampuan cetak dari mesin cetak dan mirip dengan derau yang sangat sulit diprediksi.

Proses autentikasi terdiri atas dua tahap. Pada tahap pertama, citra CDP digital didaftarkan dan dibangkitkan menggunakan sebuah pola tertentu. Citra ini kemudian dicetak pada sebuah barang dengan *printer* resmi. Lalu, tahap kedua adalah proses verifikasi. CDP yang tercetak dipindai dengan sebuah pemindai resmi, kemudian dimasukkan pada uji autentikasi berdasarkan skor kesamaan dibandingkan dengan citra yang didaftarkan. Jika lolos uji, benda tersebut dinilai autentik/asli atau dianggap sebagai CDP asli, seperti yang telah ditunjukkan pada Gambar 1.

Serangan yang paling umum pada CDP adalah mengestimasi templat digital menggunakan CDP asli yang tercetak. CDP yang tercetak dipulihkan ke versi yang paling baik untuk ditiru templat digitalnya. Terdapat beberapa metode yang digunakan dalam serangan estimasi CDP, seperti pemulihan manual menggunakan perangkat lunak pengolahan citra, restorasi Otsu, dan *deep learning*.

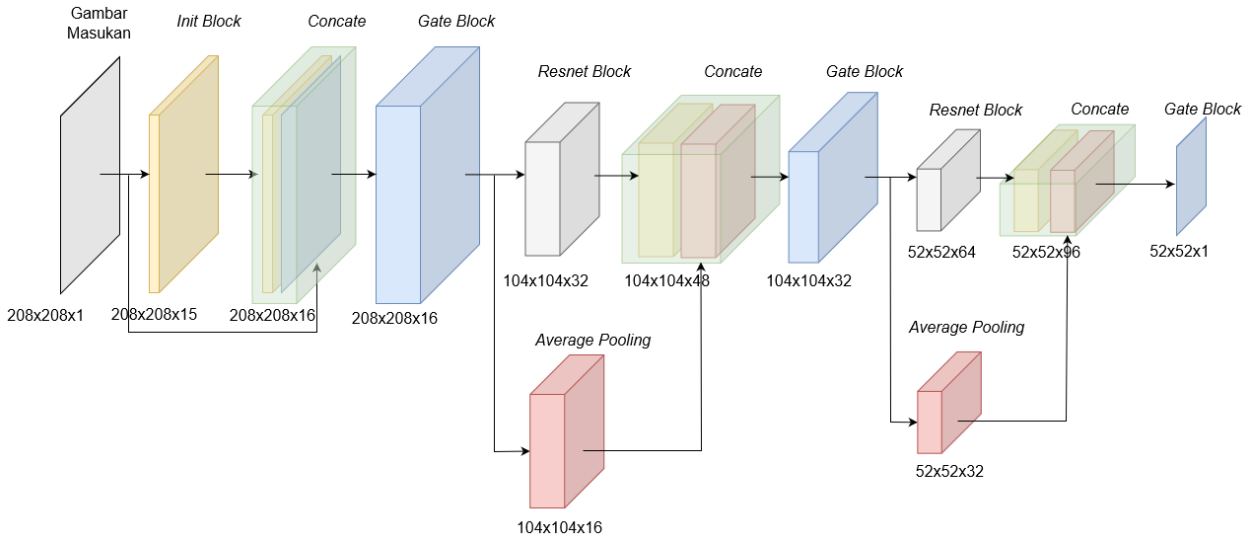
IV. METODOLOGI

A. *DATASET*

Dataset dari [14] digunakan dalam proses pengembangan model. *Dataset* ini relatif baru dan berisi 5.000 CDP unik. *Dataset* ini terdiri atas 1) hasil cetak CDP unik dan 2) hasil cetak CDP per *batch*. Semua citra dalam *dataset* berukuran 52 × 52 piksel, dengan $u = 1$ piksel per satuan dasar yang ditentukan pada 600 *pixel per inch* (ppi). CDP digital ini dicetak dengan kerapatan 600 *dot per inch* (dpi) dan dipindai dengan *printer* Canon IR-ADV C5535i 2.400 dpi, menghasilkan citra berukuran 208 × 208 piksel pada kode-kode dicetak dan dipindai dengan with $v = 4$ piksel per satuan dasar. *Dataset* pertama berisi 5.000 citra CDP asli yang unik dengan 10.000 salinan templat yng sesuai. *Dataset* kedua, yaitu *dataset batch*, dibangkitkan dengan 50 citra CDP unik, masing-masing dicetak dan dipindai 50 kali, sehingga menghasilkan basis data berisi 2.500 CDP asli dengan templat yang sesuai.

B. *MODEL YANG DIUSULKAN*

Proses C&P adalah proses yang sensitif secara spasial. Citra yang dihasilkan dari tiap proses dapat memiliki informasi yang berhubungan secara spasial. Model *deep learning* yang diusulkan akan mempertimbangkan ketergantungan spasial citra dengan menerapkan arsitektur CNN. CNN adalah sebuah



Gambar 3. Arsitektur model CDP-CNN.

algoritme *deep learning* yang mengambil citra masukan lalu menetapkan parameter (bobot pembelajaran dan *bias*) pada berbagai aspek/objek dalam citra untuk membedakan citra-citra tersebut. Model CNN menggunakan operator konvolusi spasial sebagai metode transformasi untuk menghasilkan representasi baru, yaitu citra fitur spasial. Model CNN memiliki metode ekstraksi fitur bawaan, sehingga tidak diperlukan ekstraksi fitur manual [19]. Akan tetapi, dibutuhkan lebih sedikit prapemrosesan untuk algoritme CNN, sehingga algoritme ini lebih mudah memperoleh hasil yang diinginkan dibandingkan algoritme klasifikasi yang lain.

Sebuah model CNN *deep learning* diusulkan untuk kinerja estimasi CDP yang lebih baik. CNN dipilih untuk mempertimbangkan sifat sensitif secara spasial dari proses C&P, yaitu satu piksel dapat dipengaruhi oleh nilai piksel sekitarnya. Dengan model CNN, informasi lokal yang dibutuhkan dipertahankan: algoritme CNN mereduksi suatu citra menjadi bentuk lain yang lebih mudah diproses tanpa kehilangan fitur penting dan informasi dari citra aslinya. Model yang diusulkan, CDP-CNN, memiliki tiga blok utama, yaitu *residual*, konkatenasi, dan *gating block*, seperti ditunjukkan pada Gambar 3. *Gating block* memanfaatkan konvolusi 1 × 1, yaitu tiap kanal akan memiliki karakteristiknya sendiri. Metode *gating* diterapkan sebagai mekanisme *ensemble* untuk tiap piksel dari semua kanal, karena masukan blok ini adalah konkatenasi dari blok *residual* dan blok *gating* sebelumnya. Model CDP-CNN juga memanfaatkan *skip connection* yang ditemukan dalam model ResNet [20]. *Skip connection* memungkinkan gradien lebih mudah diteruskan ke lapisan yang lebih awal dari model untuk meningkatkan proses pembelajaran pada blok *residual*.

Lapisan terakhir model memiliki dimensi spasial 52 × 52 × 1, yang sesuai dengan *ground truth* atau templat. Lapisan terakhir dilewatkan pada fungsi *binary cross-entropy loss*, karena tugasnya adalah melakukan klasifikasi biner untuk masing-masing piksel.

Dibandingkan dengan model *bottleneck* (BN) yang digunakan dalam [13], model CDP-CNN memiliki lebih sedikit parameter, yaitu 50.200 parameter, sedangkan model BN memiliki 64.800 parameter.

C. PENGATURAN EKSPERIMEN

Dataset dibagi menggunakan prosedur yang sama dengan penelitian sebelumnya [14], yaitu dengan 2.500 citra latih, 1.000 citra validasi, dan 1.500 citra uji. Pelatihan dilakukan dengan 50 *epoch* dan menggunakan *auto-finder* untuk menemukan laju pembelajaran terbaik bagi model menggunakan *library* Pytorch [21]. Adam digunakan sebagai pengoptimasi [18]. Pertama-tama, model akan belajar dari citra pelatihan, kemudian membuat prediksi pada *dataset* validasi. Model terbaik yang akan dipilih ditentukan dari kinerja model pada data validasi. Model terbaik dievaluasi pada *dataset* pengujian untuk memperoleh akurasi akhir dari model yang diusulkan. Semua program implementasi tersedia secara dalam repositori.

D. PENGUJIAN STATISTIK

Pada makalah ini, kinerja model dengan *unsharp* dan model tanpa filter *unmask* dibandingkan. Uji-t satu arah (*one tailed t-test*) digunakan untuk menyelidiki perbedaan kinerja model, signifikan atau tidak. Perbedaan margin sebesar 0,5% digunakan dengan ambang nilai-*p*, α sebesar 1%. Sampel yang digunakan dalam pengujian statistik ini adalah perbedaan BER berpasangan antara model dengan dan tanpa filter *unsharp*, yaitu $\text{diff} = \text{BER}_{\text{withoutUnsharp}} - \text{BER}_{\text{withUnsharp}}$.

Hipotesis *null*, H_0, adalah perbedaan kinerja lebih dari atau sama dengan 0,5%, sedangkan hipotesis alternatif, H_1, adalah perbedaan kinerja kurang dari 0,5%. Jika nilai-*p* kurang dari ambang yang diberikan, 1%, H_0 ditolak. Jika sebaliknya, H_0 tidak dapat ditolak.

V. HASIL EKSPERIMEN

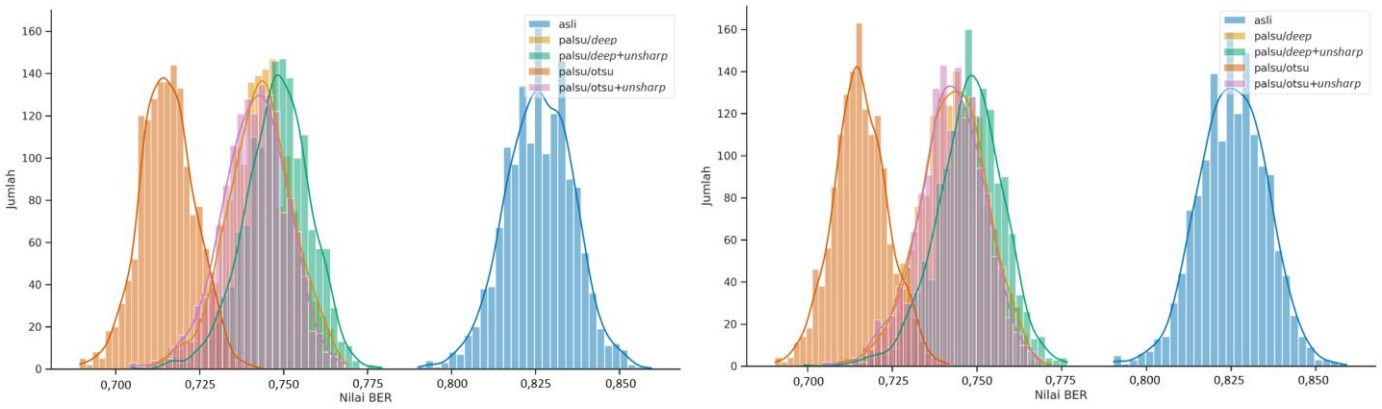
Pada bagian ini, model yang diusulkan dievaluasi. Model dilatih pada *dataset* yang sama dengan masukan prapemro

sesan yang berbeda. Dua model berbasis DL adalah model dengan masukan *unsharp mask* dan model tanpa masukan *unsharp mask*. Filter *unsharp mask* telah dibahas dalam penelitian sebelumnya [13].

A. PROSES ESTIMASI CDP

Pola CDP tercetak diestimasi menggunakan model yang diusulkan, CDP-CNN. Dari Tabel I, diketahui bahwa BER untuk model tanpa *unsharp mask* adalah 17,46% dan untuk model dengan filter *unsharp mask* adalah 17,39%. Nilai ini lebih baik daripada kinerja yang ditunjukkan dalam [13], yaitu 23,27%. Kedua kinerja model menunjukkan perbedaan statistik dengan nilai-*p* kurang dari 0,01. Hal ini berarti bahwa perbedaan antara kedua model cukup signifikan di bawah 0,5%,

p-ISSN 2301–4156 | e-ISSN 2460–5719



Gambar 4. Proses autentikasi, (a) model estimasi dengan *unsharp mask*, (b) model estimasi tanpa *unsharp mask*.

TABEL I
KINERJA SERANGAN ESTIMASI UNIK

Metode	BER	STD	Maks	Min
BN-DNN [13]	23,27%	-	26,99%	20,31%
*CDP-CNN	17,46%	1,01%	20,97%	14,09%
*CDP-CNN + *unsharp_mask*	17,39%	1,01%	21,01%	14,05%
**t-stats* = -47,37, nilai-*p* = 0,00				

TABEL II
KINERJA SERANGAN ESTIMASI *BATCH*

CDP Unik	BER	STD	Maks	Min
BN-DNN + *unsharp_mask* [13]	25,27%	0,72%	-	-
*CDP-CNN	19,64%	1,50%	26,78%	15,24%
*CDP-CNN + *unsharp_mask*	19,47%	1,53%	27,00%	15,20%
**t-stats* = -37,36, nilai- *p* = 0,00				
CDP *Batch*	**BER**	**STD**	**Maks**	**Min**
BN-DNN [14]	18,47%	0,72%	-	-
*CDP-CNN	10,36%	0,49%	11,43%	9,02%
*CDP-CNN + *unsharp_mask*	9,91%	0,62%	11,50%	8,51%
**t-stats* = -0,83, nilai-*p* = 0,2				

sehingga hipotesis *null* ditolak. Dengan demikian, pengaruh penggunaan filter prapemrosesan, *unsharp mask*, dalam estimasi CDP asli menggunakan model CDP-CNN tidak meningkatkan kinerja model secara signifikan. Dengan cara yang sama, kedua model diterapkan pada *dataset* CDP *batch*, baik pada skema estimasi individual (CDP unik) maupun CDP batch.

Dalam CDP individual atau unik pada *dataset batch*, hasil juga menunjukkan bahwa terdapat perbedaan signifikan antara model dengan dan tanpa filter *unsharp mask* kurang dari 0,5%. Di sisi lain, model dengan *unsharp mask* bekerja lebih baik daripada model tanpa filter *unsharp mask* pada estimasi CDP *batch*, dengan nilai-*p* sebesar 0,2. Hal ini berarti hipotesis *null* diterima, seperti ditunjukkan pada Tabel II. Dalam kasus ini, model dengan filter *unsharp mask* yang diterapkan pada citra masukan memiliki kinerja yang lebih baik daripada model tanpa *unsharp mask* berdasarkan uji statistik, dengan perbedaan relatif lebih dari atau sama dengan 0,5%. Oleh karena itu, model dengan *unsharp mask* dapat membantu mengestimasi pola CDP dengan skema batch.

Selain itu, semua hasil dalam eksperimen ini menghasilkan BER yang jauh lebih baik daripada hasil pada penelitian sebelumnya [13], seperti diperlihatkan dalam Tabel I dan Tabel II. Model CDP-CNN 5% lebih baik daripada penelitian sebelumnya [13] pada serangan estimasi unik dan 9% lebih baik pada serangan estimasi *batch*.

Model yang digunakan dalam makalah ini adalah model berbasis CNN, sedangkan model seblumnya menggunakan arsitektur *multi-layer perceptron* (MLP), yaitu struktur *autoencoder*. Secara umum, model CNN menunjukkan kinerja yang lebih baik daripada MLP dalam kasus pemrosesan citra, seperti memprediksi pola CDP [22]. Terlebih lagi, model CDP-CNN menggunakan lebih sedikit parameter daripada model *autoencoder* yang digunakan dalam [13], yaitu 21% lebih sedikit.

B. PROSES AUTENTIKASI CDP

Terdapat empat sumber *dataset* CDP palsu dari [13], yaitu *deep* (model BN), *deep+unsharp*, Otsu, dan Otsu+*unsharp*. *Dataset* Otsu diperoleh dari CDP asli yang dipindai, diestimasi menggunakan metode Otsu; kemudian CDP terestimasi dicetak dan dipindai. Mekanisme yang sama juga diterapkan untuk membangkitkan *dataset* lain pada metode yang berbeda. Namun, proses autentikasi yang digunakan dalam makalah ini adalah skor estimasi dari model yang digunakan dalam model estimasi CDP. Citra CDP terpindai dilewatkan pada model estimasi. Skor dihitung menggunakan skor akurasi bit total, yaitu 1 − BER. Rerata, μ, dan simpangan baku, σ, dari distribusi CDP asli dihitung untuk menentukan parameter ambang, $\epsilon = \mu - 4\sigma$, untuk membedakan antara CDP asli dan palsu. Gambar 4 menunjukkan pemisahan CDP asli dan palsu yang dihasilkan dengan metode serangan. Kedua metode, yaitu model dengan dan tanpa filter *unsharp*, menunjukkan distribusi pemisahan yang baik. Tidak ada *false positive* dan *false negative* pada pendeteksian CDP asli, menggunakan $\epsilon = \mu - 4\sigma$, sehingga model estimasi juga andal untuk digunakan sebagai metode autentikasi dalam menentukan CDP asli atau palsu.

C. DISKUSI

Dari hasil yang telah dijelaskan pada bagian sebelumnya, BER dari model terbaik adalah sekitar 10%, yang berarti masih belum memungkinkan untuk membuatnya 0%, setidaknya dengan metode yang diajukan sekarang. Dengan demikian, estimasi CDP masih tetap merupakan metode yang cukup aman untuk sistem anti-pemalsuan produk. Terlebih lagi, model CDP-CNN yang dilatih mengandung informasi tentang kualitas citra CDP dari proses pelatihan, sehingga cocok digunakan sebagai metode autentikasi. Selain itu, model berbasis CNN

lebih diimplementasikan pada masukan berupa citra daripada ekstraksi fitur manual dengan *classifier* tertentu.

Akan tetapi, terdapat batasan-batasan pada metode yang diusulkan. Metode ini hanya diuji pada tipe khusus peranti (sebuah *printer* dan *scanner*/pemindai) dan kemungkinan tidak bekerja dengan baik pada peranti lain. Oleh karena itu, model perlu diuji pada peranti-peranti yang berbeda untuk memastikan efektivitasnya di dunia nyata, karena pada proses produksi, peranti yang digunakan oleh pengguna tidak dapat dikendalikan.

VI. KESIMPULAN

Sebuah model estimasi CDP berbasis arsitektur CNN telah diusulkan. Model yang diusulkan secara efektif bekerja lebih baik pada *dataset* yang sama dengan *dataset* pada penelitian sebelumnya, dengan metrik akurasi yang lebih baik (BER yang lebih kecil) dan proses pelatihan yang lebih efisien dengan lebih sedikit parameter. Penggunaan arsitektur CNN juga dapat mengesampingkan kebutuhan implementasi *unsharp masking* yang terbukti tidak signifikan dengan uji statistik-t satu arah. Namun, filter *unsharp mask* secara signifikan mengurangi BER, sebesar paling tidak 0,5%, pada serangan estimasi *batch*. Model estimasi CDP-CNN 5% lebih baik daripada model sebelumnya pada serangan estimasi unik dan 9% lebih baik pada serangan estimasi *batch*. Selanjutnya, metode autentikasi menggunakan skor dari model estimasi, yang memiliki pemisahan yang sangat baik untuk membedakan CDP asli dari yang palsu. Oleh karena itu, satu model dapat digunakan untuk dua tugas sekaligus, yaitu estimasi dan autentikasi. BER model yang diusulkan adalah 9,91% pada estimasi CDP *batch*. Hal ini dapat meningkatkan *false positive* proses autentikasi. Namun, di masa mendatang, model khusus autentikasi berbasis DL mungkin diperlukan untuk meningkatkan pemisahan distribusi CDP asli dan palsu.

KONFLIK KEPENTINGAN

Penulis menyatakan bahwa tidak ada konflik kepentingan dalam makalah berjudul "Model Berbasis CNN untuk Estimasi dan Autentikasi Copy Detection Pattern" ini.

UCAPAN TERIMA KASIH

Terima kasih diucapkan kepada Yusuf Helmy Hensyaputra atas bantuannya dalam merevisi makalah ini dan mengawasi hasil eksperimen.

KONTRIBUSI PENULIS

Konseptualisasi, Syukron Abu Ishaq Alfarozi dan Azkario Rizky Pratama; metodologi, Syukron Abu Ishaq Alfarozi; eksprerimen dan simulasi, Syukron Abu Ishaq Alfarozi; validasi, Syukron Abu Ishaq Alfarozi dan Azkario Rizky Pratama; analisis formal, Syukron Abu Ishaq Alfarozi dan Azkario Rizky Pratama; investigasi, Syukron Abu Ishaq Alfarozi dan Azkario Rizky Pratama; sumber daya, Syukron Abu Ishaq Alfarozi; kurasi data, Syukron Abu Ishaq Alfarozi; penulisan—penyusuan draf asli, Syukron Abu Ishaq Alfarozi; penulisan—peninjauan dan penyuntingan, Syukron Abu Ishaq Alfarozi dan Azkario Rizky Pratama.

REFERENSI

[1] E. Gasiorowski-Denis (2014) "Crackdown on counterfeiting," [Online], https://www.iso.org/news/2014/01/Ref1809.html, tanggal akses: 26-Jul-2022.

[2] L. Korsell, "Fraud in the Twenty-first Century," *Eur. J. Crim. Policy Res.*, Vol. 26, hal. 285–291, Sep. 2020, doi: 10.1007/s10610-020-09463-2.

[3] OEICD/EUIPO (2016) "Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact," [Online], https://read.oecd-ilibrary.org/governance/trade-in-counterfeit-and-pirated-goods_9789264252653-en#page5, tanggal akses: 26-Jul-2022.

[4] A. Anderson (2006) "Combating Counterfeiting: Simple Steps You Can Take Now to Protect Your Brand from Piracy," [Online], https://www.hollandhart.com/articles/CounterfeitingArticleAndersonRev2.pdf, tanggal akses: 26-Jul-2022.

[5] J. Picard, "Digital Authentication with Copy-Detection Patterns," *Proc. Vol. 5310 Opt. Secur. Counterfeit Deterrence Tech. V*, R.L. van Renesse, Ed., Jun. 2004, hal. 176–183, doi: 10.1117/12.528055.

[6] C. Chen dkk., "A Copy-Proof Scheme Based on the Spectral and Spatial Barcoding Channel Models," *IEEE Trans. Inf. Forensics Secur.*, Vol. 15, hal. 1056–1071, Agu. 2019, doi: 10.1109/TIFS.2019.2934861.

[7] I.H. Sarker, "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions," *SN Comput. Sci.*, Vol. 2, hal. 1-20, Agu. 2021, doi: 10.1007/s42979-021-00815-1.

[8] P.R. Kumar dan E.B.K. Manash, "Deep Learning: A Branch of Machine Learning," *J. Phys. Conf. Ser.*, Vol. 1228, hal. 1-9, 2019, doi: 10.1088/1742-6596/1228/1/012045.

[9] K. Choudhary dkk., "Recent Advances and Applications of Deep Learning Methods in Materials Science," *npj Comput. Mater.*, Vol. 8, hal. 1-26, Apr. 2022, doi: 10.1038/s41524-022-00734-6.

[10] V. Kober, T. Choi, V. Diaz-Ramírez, dan P. Aguilar-González, "Pattern Recognition: Recent Advances and Applications," *Math. Probl. Eng.*, Vol. 2018, hal. 1-2, Nov. 2018, doi: 10.1155/2018/8510319.

[11] B. Liu dan J. Liu, "Overview of Image Denoising Based on Deep Learning," *J. Phys. Conf. Ser.*, Vol. 1176, No. 2, hal. 1-6, 2019, doi: 10.1088/1742-6596/1176/2/022010.

[12] K. Yun, A. Huyen, dan T. Lu, "Deep Neural Networks for Pattern Recognition," 2018, *arXiv:1809.09645*.

[13] E. Khermaza, I. Tkachenko, dan J. Picard, "Can Copy Detection Patterns be Copied? Evaluating the Performance of Attacks and Highlighting the Role of the Detector," *2021 IEEE Int. Work. Inf. Forensics Secur. (WIFS)*, 2021, hal. 1-6, doi: 10.1109/WIFS53200.2021.9648384.

[14] P. Zhang, W. Zhang, dan N. Yu, "Copy Detection Pattern-Based Authentication for Printed Documents with Multi-Dimensional Features," *2019 7th Int. Conf. Inf. Commun., Networks (ICICN)*, 2019, hal. 150–157, doi: 10.1109/ICICN.2019.8834939.

[15] O. Taran dkk., "Mobile Authentication of Copy Detection Patterns: How Critical Is to Know Fakes?" *2021 IEEE Int. Work. Inf. Forensics Secur. (WIFS)*, 2021, hal. 1-6, doi: 10.1109/WIFS53200.2021.9648398.

[16] R. Chaban dkk., "Machine Learning Attack on Copy Detection Patterns: Are 1 × 1 Patterns Cloneable?" *2021 IEEE Int. Work. Inf. Forensics Secur. (WIFS)*, 2021, hal. 1-6, doi: 10.1109/WIFS53200.2021.9648387.

[17] O. Taran, S. Bonev, dan S. Voloshynovskiy, "Clonability of Anti-Counterfeiting Printable Graphical Codes: A Machine Learning Approach," *ICASSP 2019, 2019 IEEE Int. Conf. Acoust. Speech, Signal Process.*, 2019, hal. 2482–2486, doi: 10.1109/ICASSP.2019.8682967.

[18] D.P. Kingma dan J.L. Ba, "Adam: A Method for Stochastic Optimization," 2017, arXiv:1412.6980v9.

[19] S. Saidah, I.P.Y.N. Suparta, dan E. Suhartono, "Modifikasi Convolutional Neural Network Arsitektur GoogLeNet dengan Dull Razor Filtering untuk Klasifikasi Kanker Kulit," *J. Nas. Tek. Elektro, Teknol. Inf.*, Vol. 11, No. 2, hal. 148–153, Mei 2022, doi: 10.22146/jnteti.v11i2.2739.

[20] K. He, X. Zhang, S. Ren, dan J. Sun, "Deep Residual Learning for Image Recognition," *2016 IEEE Comput. Vis. Pattern Recognit.*, 2016, hal. 770–778, doi: 10.1109/CVPR.2016.90.

[21] A. Paszke dkk., "PyTorch: An Imperative Style, High-Performance Deep Learning Library," dalam *NIPS,19: Proceedings of the 33rd International Conference on Neural Information Processing Systems*, H.M. Wallach dkk., Eds., Red Hook, NY, USA: Curran Associates Inc., 2019, hal. 8026–8037.

[22] Y. LeCun, L. Bottou, Y. Bengio, dan P. Haffner, "Gradient-Based Learning Applied to Document Recognition," *Proc. IEEE*, Vol. 86, No. 11, hal. 2278–2324, Nov. 1998, doi: 10.1109/5.726791.