Verificação da Autenticidade de Assinaturas Manuscritas Utilizando Redes Neurais Convolucionais

Defesa do Trabalho de Conclusão de Curso II

por

Marcos Wenneton V. de Araujo

Orientadora: Elloá B. Guedes

{mwvda.eng, ebgcosta}@uea.edu.br

do

Grupo de Pesquisa em Sistemas Inteligentes
Escola Superior de Tecnologia
Universidade do Estado do Amazonas

Manaus – Amazonas – Brasil

6 de dezembro de 2019

Agenda

1. Introdução
2. Objetivos
3. Justificativa
4. Metodologia
5. Cronograma
6. Fundamentação Teórica
7. Solução Proposta
8. Resultados e Discussões
9. Considerações Finais
10. Referências

Agenda

Verificação de autenticidade

- Segurança em sistemas computacionais
- Biometria
  - Características fisiológicas
  - Traços comportamentais
- Assinaturas manuscritas como forma de biometria
  - Utilização desde os tempos primórdios
  - Método não-invasivo
  - Baixo custo de aquisição
  - Difícil verificação de autenticidade devido a grande variabilidade dos padrões encontrados nas assinaturas

Agenda

Objetivos

Objetivo Geral

Verificar a autenticidade de assinaturas manuscritas utilizando Redes Neurais Convolucionais

Objetivos

Objetivo Geral

Verificar a autenticidade de assinaturas manuscritas utilizando Redes Neurais Convolucionais

Objetivos Específicos

- Realizar a fundamentação teórica acerca dos conceitos das redes neurais convolucionais;
- Consolidar uma base de dados representativa de assinaturas manuscritas;
- Descrever o problema considerado segundo uma tarefa de Aprendizado de Máquina;
- Propor, treinar e testar diferentes redes neurais convolucionais para a tarefa considerada;
- Analisar os resultados obtidos.

Agenda

Justificativa

- Autenticação de assinaturas manuscritas
  - Ampla utilização em **documentos oficiais** e **transações financeiras** atualmente
  - Pode ser utilizada em documentos e obras de arte históricas

- Redes Neurais Convolucionais
  - Prática de conceitos, técnicas e tecnologias de uma área emergente da Computação
  - Proposta alinhada com as atividades desenvolvidas pelo **Laboratório de Sistemas Inteligentes**

Agenda

Metodologia

A condução das atividades obedece à metodologia apresentada a seguir, composta dos seguintes passos:

1. Estudo dos conceitos relacionados à Aprendizado de Máquina, Redes Neurais Convolucionais e *Deep Learning*;
2. Descrição do problema considerado como uma tarefa de Aprendizado de Máquina;
3. Consolidação de uma base de dados representativa de assinaturas originais e forjadas;
4. Levantamento do ferramental tecnológico para implementação das redes neurais convolucionais;
5. Proposição de modelos de redes neurais convolucionais para o problema considerado, contemplando arquitetura, parâmetros e hiperparâmetros;

Metodologia

6. Treino das redes propostas para a tarefa de aprendizado considerada;
7. Teste das redes previamente treinadas com vistas a coleta de métricas de desempenho;
8. Análise dos resultados e identificação dos modelos mais adequados para o problema considerado;
9. Escrita da proposta de Trabalho de Conclusão de Curso;
10. Defesa da proposta de Trabalho de Conclusão de Curso;
11. Escrita do Trabalho de Conclusão de Curso; e
12. Defesa do Trabalho de Conclusão de Curso.

Agenda

Cronograma

Tabela 1: Cronograma de atividades

	2019										
	02	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**
Atividade 1	X	X	X								
Atividade 2		X									
Atividade 3		X	X								
Atividade 4			X								
Atividade 5				X	X	X	X				
Atividade 6				X	X	X	X				
Atividade 7							X	X			
Atividade 8									X	X	
Atividade 9	X	X	X	X	X						
Atividade 10					X						
Atividade 11						X	X	X	X	X	X
Atividade 12											X

Agenda

Aprendizado de Máquina

- Algoritmos capazes de aprender padrões por meio de exemplos, baseando-se em dados previamente disponíveis
- As técnicas de **Aprendizado de Máquina** têm sido aplicadas com sucesso em um grande número de problemas reais em diversos domínios
- Características: natureza inferencial e a boa capacidade de generalização
- Paradigmas de aprendizado supervisionado e não-supervisionado

Redes Neurais Artificiais

- Inspiradas na capacidade de processamento de informações do cérebro humano

- **Neurônios artificiais** são as unidades fundamentais de uma RNA
- **Função de ativação** fornece a resposta de um neurônio para uma dada entrada

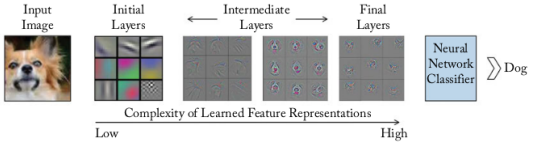
- Neurônios artificiais são conectados entre si na forma de uma rede e distribuídos em uma ou mais camadas ocultas

- Algoritmo *Backpropagation*
  - Fase *forward* – produz uma saída para uma dada entrada
  - Fase *backwards* – calcula a diferença entre as saídas para minimizar o erro

Deep Learning e Redes Neurais Convolucionais

- *Deep Learning* é uma subárea específica do Aprendizado de Máquina
- Redes Neurais Convolucionais (CNNs):
  - Possuem camadas **hierárquicas** e **profundas**
  - Aproveitam-se da operação matemática denominada **convolução**
  - Destacam-se pelo reconhecimento de padrões em dados de alta dimensionalidade

Figura 1: Papel das camadas convolucionais e *feature maps* das CNNs



Arquiteturas Canônicas de Redes Neurais Convolucionais

- Arquiteturas com bom desempenho em competições de **Visão Computacional**
- Comuns ainda hoje no cenário de *Deep Learning*

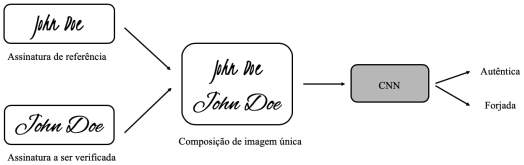
- LeNet (1998)
- AlexNet (2012)
- VGG (2014)
- Inception (2014)
- ResNet (2015)

Agenda

Tarefa de Aprendizado

- Problema abordado como uma **tarefa de classificação binária**
- **Entrada:**
  - Imagem em escala de cinza com dimensões de 256×256 *pixels* contendo duas assinaturas manuscritas (uma de referência e outra para a inferência)
- **Saída:**
  - Classificação da assinatura quanto à sua autenticidade (autêntica ou forjada)

Figura 2: Visão geral da tarefa de aprendizado considerada



Tarefa de Aprendizado

- Partição dos exemplos utilizando o método *holdout*
  - 70% para treinamento;
  - 10% para validação;
  - 20% para teste.

- Utilização das métricas Acurácia, *F-score* e EER (*equal error rate*) para análise de desempenho dos modelos

Coleta do conjunto de Dados

- *Signature Verification Competition* 2009 (SigComp2009)
- Dois conjuntos de dados foram utilizados na competição:
  - *Norwegian Information Security Donders Centre for Cognition* (NISDCC)
  - *Netherlands Forensic Institute* (NFI)
- Informações *online* e *offline* das assinaturas

Tabela 2: Quantitativo de indivíduos e assinaturas *offline* por conjunto de dados.

Conjunto	Autores originais	Autores forjadores	Autores originais com assinaturas forjadas	Assinaturas genuínas	Assinaturas forjadas	Total de assinaturas
NISDCC	12	31	12	60	1.838	1.898
NFI	79	33	19	940	624	1.564

Preparação dos Dados

- Combinação e redimensionamento das imagens
- Abordagem A
  - Separação dos exemplos **autênticos** conforme o método *holdout*
  - Exemplos **forjados** necessitaram de um diferente tipo de separação
  - Boa para a identificação da falsificação de assinaturas de autores já visto pelos modelos
- Abordagem B
  - Separação do **quantitativo de autores** para cada etapa conforme método *holdout*
  - Boa para a identificação de autores inéditos para o modelo

Preparação dos Dados

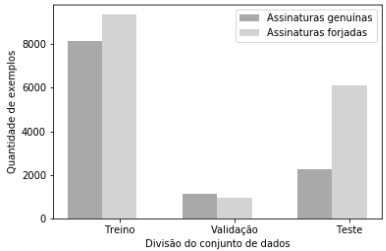
Tabela 3: Quantitativo de exemplos por finalidade na tarefa de aprendizado considerada e classe para cada abordagem.

Conjunto	Tipo de Exemplo	Abordagem A		Abordagem B	
		Nº de Exemplos	Proporção	Nº de Exemplos	Proporção
Treinamento	Autêntico	9.374	54%	8.072	43%
	Forjado	8.131	46%	10.887	57%
Validação	Autêntico	947	46%	1.179	37%
	Forjado	1.134	54%	1.976	63%
Teste	Autêntico	2.257	27%	2.271	39%
	Forjado	6.119	73%	3.577	61%

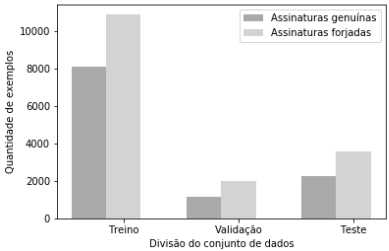
Preparação dos Dados

Figura 3: Representação gráfica da proporção dos exemplos por classe e finalidade para as abordagens na tarefa de aprendizado considerada.

(a) Abordagem A



(b) Abordagem B



- Normalização dos *pixels* das imagens ao serem fornecidas às CNNs

Modelos, Parâmetros e Hiperparâmetros Utilizados

- Arquiteturas de CNNs escolhidas: LeNet, AlexNet, MobileNet, ShuffleNet, SqueezeNet, VGG-16 e InceptionV3

Tabela 4: Valores dos hiperparâmetros selecionados para a elaboração dos modelos.

Épocas	*Patience*	Otimizador	Função de ativação
200	5, 10 e 15	SGD, Adam e RMSprop	ReLU, ELU, SELU e Leaky ReLU

- Busca em *grid* nos hiperparâmetros quando possível
- Demais casos, hiperparâmetros típicos

Agenda

Resultados Finais

- Utilização de um servidor para treinamento das CNNs:
  - Processador Intel Core i7
  - 16 GB de RAM
  - GPU Nvidia GeForce GTX 1080 com 11 GB de memória
- Modelos degenerados tiveram seus resultados descartados
  - *Dying ReLU problem*
  - Permanência em mínimos locais no treinamento

LeNet

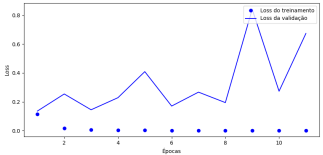
Tabela 5: Detalhamento dos melhores resultados obtidos com a arquitetura LeNet.

Abordagem	**Otimizador**	***Patience***	**Função de Ativação**	**Acurácia**	***F-Score***	**EER**
Abordagem A	RMSprop	5	ReLU	0.9865	0.9755	1.1679
Abordagem B	Adam	10	ELU	0.8361	0.8159	12.5245

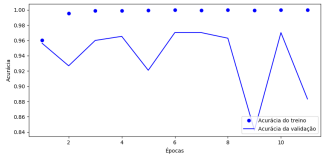
LeNet

Figura 5: Histórico de *loss* e acurácia durante o treinamento dos melhores modelos obtidos com a arquitetura LeNet.

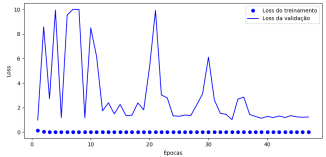
(a) *Loss* LeNet A.



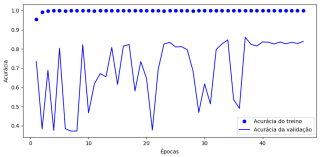
(b) Acurácia LeNet A.



(c) *Loss* LeNet B.



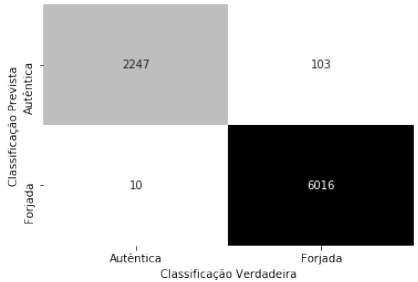
(d) Acurácia LeNet B.



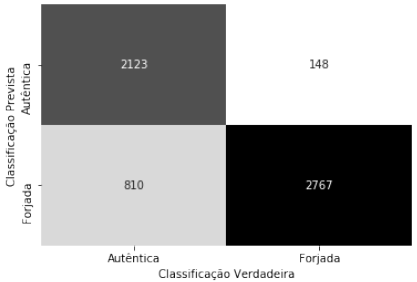
LeNet

Figura 7: Matrizes de confusão dos melhores modelos obtidos com a arquitetura LeNet.

(a) LeNet A



(b) LeNet B



AlexNet

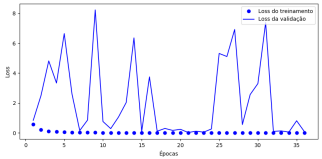
Tabela 6: Detalhamento dos melhores modelos obtidos com a arquitetura AlexNet para cada uma das abordagens consideradas neste trabalho.

Abordagem	Otimizador	*Patience*	Função de Ativação	Acurácia	F-Score	EER
Abordagem A	Adam	15	ELU	0.9654	0.9393	1.5401
Abordagem B	RMSprop	5	ELU	0.8593	0.7993	13.8265

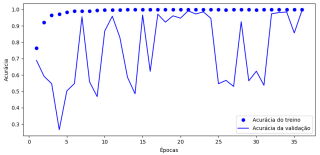
AlexNet

Figura 9: Histórico de *loss* e acurácia durante o treinamento dos melhores modelos obtidos com a arquitetura AlexNet.

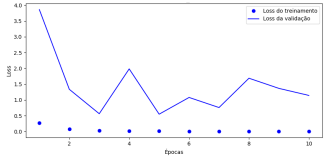
(a) *Loss* AlexNet A.



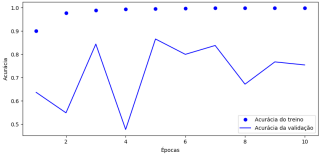
(b) Acurácia AlexNet A.



(c) *Loss* AlexNet B.



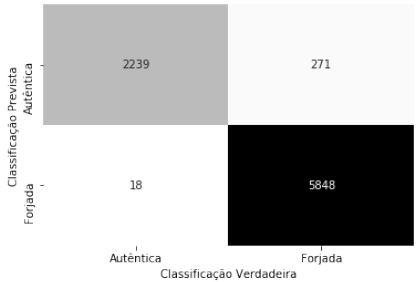
(d) Acurácia AlexNet B.



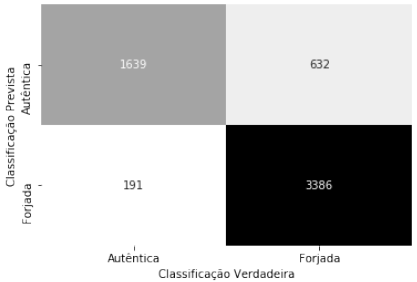
AlexNet

Figura 11: Matrizes de confusão dos melhores modelos obtidos com a arquitetura AlexNet.

(a) AlexNet A



(b) AlexNet B



MobileNet

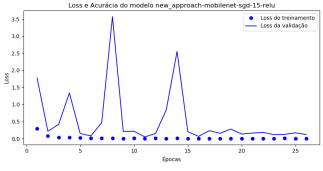
Tabela 7: Detalhamento dos melhores modelos obtidos com a arquitetura MobileNet para cada uma das abordagens consideradas neste trabalho.

Abordagem	Otimizador	*Patience*	Função de Ativação	Acurácia	F-Score	EER
Abordagem A	SGD	15	ReLU	0.9606	0.9318	0.9304
Abordagem B	Adam	15	ReLU	0.8856	0.8658	9.9475

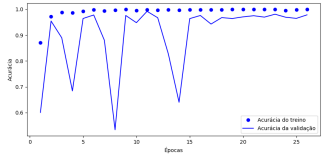
MobileNet

Figura 13: Histórico de *loss* e acurácia durante o treinamento dos melhores modelos obtidos com a arquitetura MobileNet.

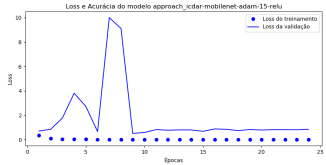
(a) *Loss* MobileNet A.



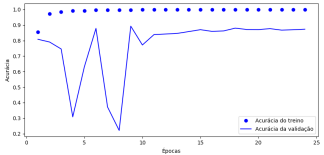
(b) Acurácia MobileNet A.



(c) *Loss* MobileNet B.



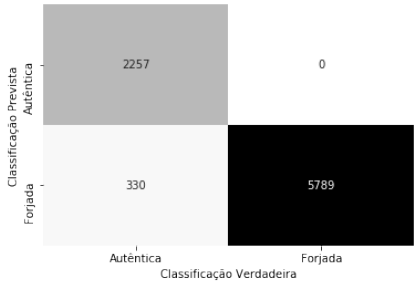
(d) Acurácia MobileNet B.



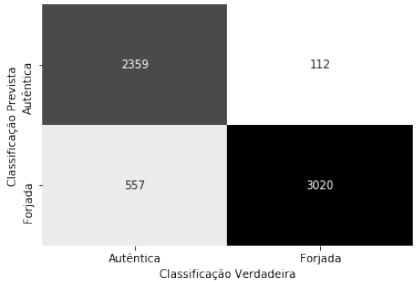
MobileNet

Figura 15: Matrizes de confusão dos melhores modelos obtidos com a arquitetura MobileNet.

(a) MobileNet A



(b) MobileNet B



ShuffleNet

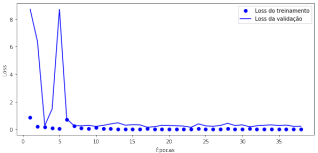
Tabela 8: Detalhamento dos modelos obtidos com a arquitetura ShuffleNet para cada uma das abordagens consideradas.

Abordagem	Otimizador	*Patience*	Função de Ativação	Acurácia	F-Score	EER
Abordagem A	RMSprop	15	ReLU	0.9404	0.9004	7.5400
Abordagem B	RMSprop	15	ReLU	0.8345	0.7705	23.8151

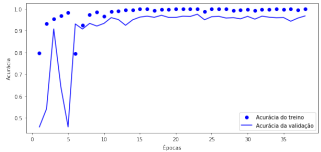
ShuffleNet

Figura 17: Histórico de *loss* e acurácia durante o treinamento dos modelos obtidos com a arquitetura ShuffleNet.

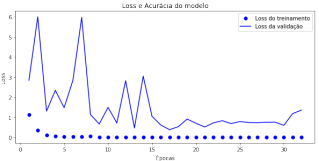
(a) *Loss* ShuffleNet A.



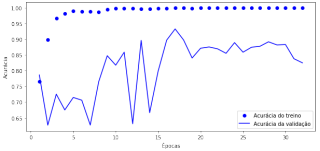
(b) Acurácia ShuffleNet A.



(c) *Loss* ShuffleNet B.



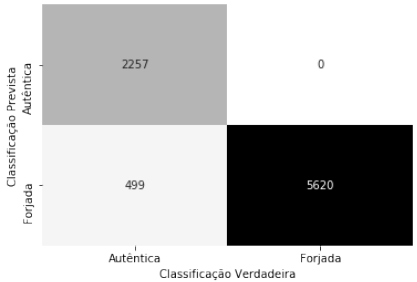
(d) Acurácia ShuffleNet B.



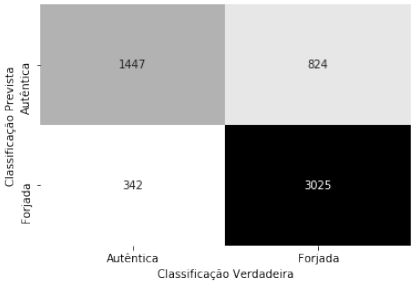
ShuffleNet

Figura 19: Matrizes de confusão dos modelos obtidos com a arquitetura ShuffleNet.

(a) ShuffleNet A



(b) ShuffleNet B



SqueezeNet

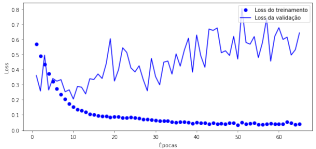
Tabela 9: Detalhamento dos modelos obtidos com a arquitetura SqueezeNet para cada uma das abordagens consideradas neste trabalho.

Abordagem	Otimizador	*Patience*	Função de Ativação	Acurácia	F-Score	EER
Abordagem A	RMSprop	15	ReLU	0.9048	0.8948	11.5074
Abordagem B	RMSprop	15	ReLU	0.8210	0.7709	20.1673

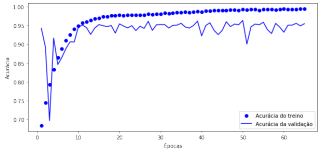
SqueezeNet

Figura 21: Histórico de *loss* e acurácia durante o treinamento dos modelos obtidos com a arquitetura SqueezeNet.

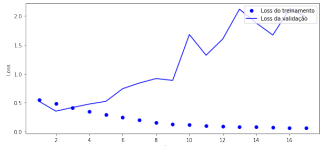
(a) *Loss* SqueezeNet A.



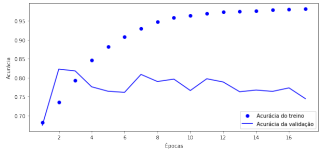
(b) Acurácia SqueezeNet A.



(c) *Loss* SqueezeNet B.



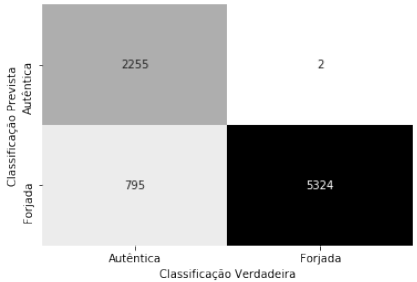
(d) Acurácia SqueezeNet B.



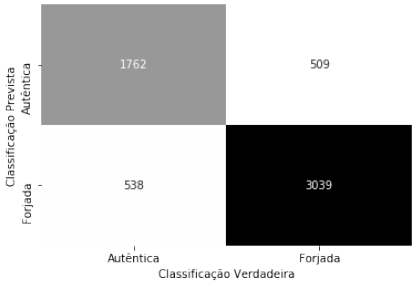
SqueezeNet

Figura 23: Matrizes de confusão dos modelos obtidos com a arquitetura SqueezeNet.

(a) SqueezeNet A



(b) SqueezeNet B



VGG-16

- Treinada apenas para abordagem B, com hiperparâmetros *Ad Hoc*

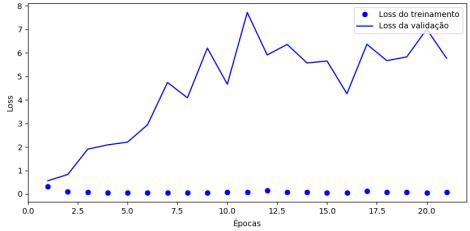
Tabela 10: Detalhamento do modelo obtido com a arquitetura VGG-16 para a abordagem B.

Otimizador	*Patience*	Função de Ativação	Acurácia	F-Score	EER
RMSprop	10	ELU	0.8391	0.8019	16.1096

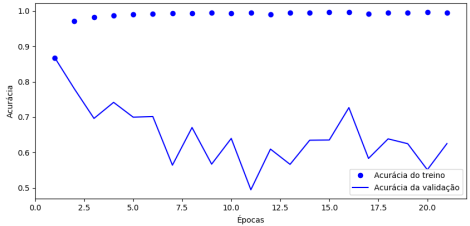
VGG-16

Figura 25: Histórico de *loss* e acurácia durante o treinamento do modelo obtido com a arquitetura VGG-16.

(a) *Loss* VGG-16 B.

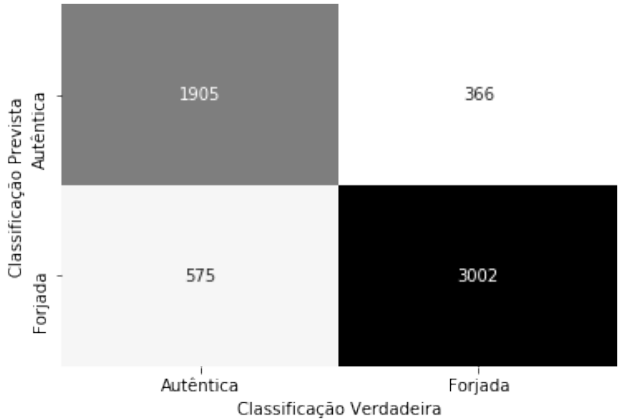


(b) Acurácia VGG-16 B.



VGG-16

Figura 27: Matriz de confusão do modelo obtido com a arquitetura VGG-16.



InceptionV3

- Treinada apenas para abordagem B, com hiperparâmetros *Ad Hoc*

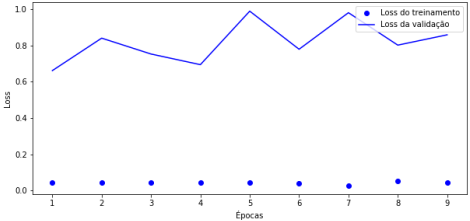
Tabela 11: Detalhamento do modelo obtido com a arquitetura Inception-V3 para a abordagem B.

Otimizador	*Patience*	Função de Ativação	Acurácia	F-Score	EER
RMSprop	5	ELU	0.8394	0.8070	16.9493

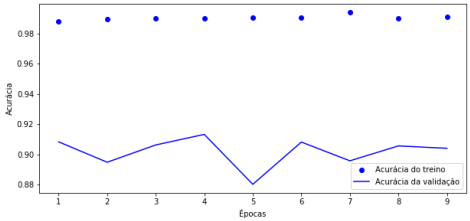
InceptionV3

Figura 28: Histórico de *loss* e acurácia durante o treinamento do modelo obtido com a arquitetura InceptionV3.

(a) *Loss* InceptionV3 B.

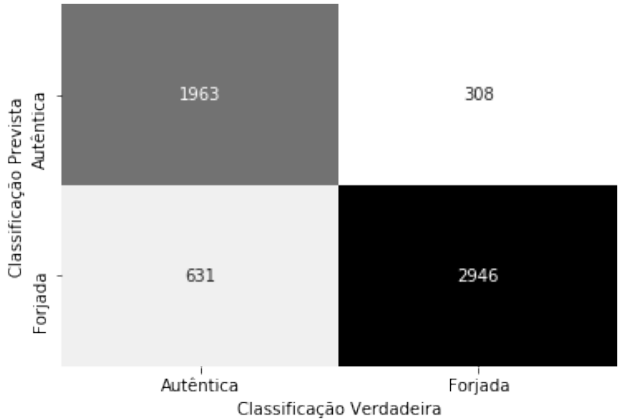


(b) Acurácia InceptionV3 B.



InceptionV3

Figura 30: Matriz de confusão do modelo obtido com a arquitetura InceptionV3.



Agenda

Considerações Finais

- 222 redes foram treinadas e testadas com um total de 27.962 exemplos

Considerações Finais

- 222 redes foram treinadas e testadas com um total de 27.962 exemplos

- Melhor desempenho Abordagem A: LeNet
  - **Parâmetros e Hiperparâmetros**: Otimizador RMSprop, *patience* 5 e função de ativação *Leaky* ReLU.
  - **Acurácia**: 0.9865
  - ***F-Score***: 0.9755
  - **EER**: 1.17%

Considerações Finais

- 222 redes foram treinadas e testadas com um total de 27.962 exemplos
- Melhor desempenho Abordagem A: LeNet
  - **Parâmetros e Hiperparâmetros**: Otimizador RMSprop, *patience* 5 e função de ativação *Leaky* ReLU.
  - **Acurácia**: 0.9865
  - ***F-Score***: 0.9755
  - **EER**: 1.17%
- Melhor desempenho Abordagem B: MobileNet
  - **Parâmetros e Hiperparâmetros**: Otimizador Adam, *patience* 15 e função de ativação ReLU.
  - **Acurácia**: 0.8856
  - ***F-Score***: 0.8658
  - **EER**: 9.94%

Considerações Finais

- Trabalhos futuros:
  - Encontrar modelos mais compactos
  - Remoção de mapas de calor afim de ajudar na checagem de assinaturas por revisores humanos

Agenda

1. Introdução
2. Objetivos
3. Justificativa
4. Metodologia
5. Cronograma
6. Fundamentação Teórica
7. Solução Proposta
8. Resultados e Discussões
9. Considerações Finais
10. Referências

Referências

- BRAGA, A. de P.; CARVALHO, A. P. de Leon F. de; LUDERMIR, T.B. *Redes Neurais Artificiais: Teorias e Aplicações*. Rio de Janeiro, RJ: Livros Técnicos e Científicos Editora S.A., 2000.

- BLANKERS, V. L. et al. *The icdar 2009 signature verification competition*. In: *10th International Conference on Document Analysis and Recognition*. Barcelona, Catalonia, Spain: IEEE, 2009. p. 1403-1407.

- KHAN, S. et. al. *A Guide to Convolutional Neural Networks for Computer Vision*. Austrália: Morgan & Claypool, 2018.

- LIWICKI, M. *IAPR TC11 - ICDAR 2009 Signature Verification Competition (SigComp2009)*. 2012. Disponível em: hhttp://www.iapr-tc11.org/mediawiki/index.php?title=IAPR-TC11:Reading Systemsi. Acesso em 5 de março de 2019.

Verificação da Autenticidade de Assinaturas Manuscritas Utilizando Redes Neurais Convolucionais

Defesa do Trabalho de Conclusão de Curso II

por

Marcos Wenneton V. de Araujo

Orientadora: Elloá B. Guedes

{mwvda.eng, ebgcosta}@uea.edu.br

do

Grupo de Pesquisa em Sistemas Inteligentes
Escola Superior de Tecnologia
Universidade do Estado do Amazonas

Manaus – Amazonas – Brasil