Verificação da Autenticidade de Assinaturas Manuscritas Utilizando Redes Neurais Convolucionais

Defesa do Trabalho de Conclusão de Curso I

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

17 de junho de 2019

Agenda

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

Agenda

1. Introdução

2. Objetivos

3. Justificativa

4. Metodologia

5. Cronograma

6. Fundamentação Teórica

7. Solução Proposta

8. Resultados Parciais

9. Considerações Finais

10. Referências

Assinaturas manuscritas

- 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

1. Introdução

2. Objetivos

3. Justificativa

4. Metodologia

5. Cronograma

6. Fundamentação Teórica

7. Solução Proposta

8. Resultados Parciais

9. Considerações Finais

10. Referências

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

1. Introdução

2. Objetivos

3. Justificativa

4. Metodologia

5. Cronograma

6. Fundamentação Teórica

7. Solução Proposta

8. Resultados Parciais

9. Considerações Finais

10. Referências

Justificativa

- Autenticação de assinaturas manuscritas
  - Devido a ampla utilização em documentos oficiais e transações financeiras atualmente, busca-se a melhoria e avaliação de métodos para este fim;
  - Documentos e obras de arte históricas.
- Prática de conceitos, técnicas e tecnologias de uma área emergente da Computação
- Proposta alinhada com as atividades desenvolvidas pelo **Laboratório de Sistemas Inteligentes**

Agenda

1. Introdução

2. Objetivos

3. Justificativa

4. Metodologia

5. Cronograma

6. Fundamentação Teórica

7. Solução Proposta

8. Resultados Parciais

9. Considerações Finais

10. Referências

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

1. Introdução

2. Objetivos

3. Justificativa

4. Metodologia

5. Cronograma

6. Fundamentação Teórica

7. Solução Proposta

8. Resultados Parciais

9. Considerações Finais

10. Referências

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

1. Introdução

2. Objetivos

3. Justificativa

4. Metodologia

5. Cronograma

6. Fundamentação Teórica

7. Solução Proposta

8. Resultados Parciais

9. Considerações Finais

10. Referências

Aprendizado de Máquina

- 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 dos métodos e técnicas desta área
- Algoritmos capazes de aprender padrões por meio de exemplos, baseado-se em dados previamente disponíveis
- 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

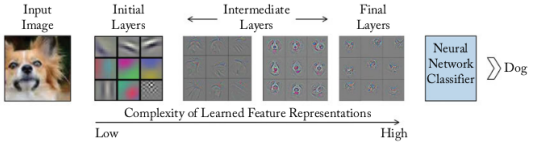
- Neurônios artificiais são conectados entre si na forma de uma rede e distribuídos em uma ou mais camadas ocultas

- Algoritmo *Backpropagation*
  - Fase *foward* – 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

- 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

1. Introdução

2. Objetivos

3. Justificativa

4. Metodologia

5. Cronograma

6. Fundamentação Teórica

7. Solução Proposta

8. Resultados Parciais

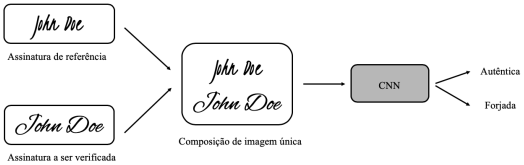
9. Considerações Finais

10. Referências

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

- Utilização das métricas Acurácia e *F-score* 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

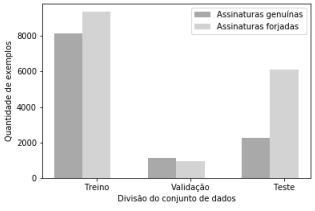
- Separação dos exemplos autênticos conforme o método *holdout*
- Exemplos forjados necessitaram de um diferente tipo de separação

Tabela 3: Quantitativo de exemplos.

Conjunto	Tipo de Exemplo	Quantidade de Dados	Proporção
Treinamento	Autêntico	9.374	54%
	Forjado	8.131	46%
Validação	Autêntico	947	46%
	Forjado	1.134	54%
Teste	Autêntico	6.119	73%
	Forjado	2.257	27%

Preparação dos Dados

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



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

Modelos, Parâmetros e Hiperparâmetros Utilizados

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

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

1. Introdução

2. Objetivos

3. Justificativa

4. Metodologia

5. Cronograma

6. Fundamentação Teórica

7. Solução Proposta

8. Resultados Parciais

9. Considerações Finais

10. Referências

Resultados Parciais

- 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

- **LeNet** e **AlexNet**

- Modelos degenerados tiveram seus resultados descartados
  - *Dying ReLU problem*
  - Permanência em mínimos locais no treinamento

LeNet

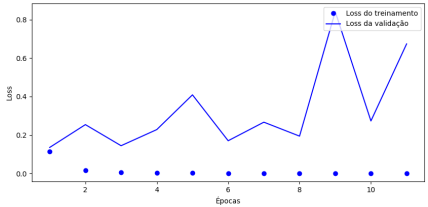
Tabela 5: Detalhamento dos melhores modelos obtidos com a arquitetura LeNet.

Identificação	Otimizador	*Patience*	Função de Ativação	Acurácia	F-Score
LeNet A	RMSprop	5	*Leaky* ReLU	0.9865	0.9755
LeNet B	RMSprop	15	ReLU	0.9858	0.9740
LeNet C	SGD	5	ELU	0.9787	0.9619
LeNet D	RMSprop	10	SELU	0.9707	0.9483

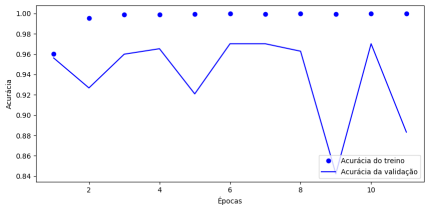
LeNet

Figura 4: Histórico de *loss* e acurácia durante o treinamento dos melhores modelos obtidos com a arquitetura LeNet.

(a) *Loss* durante o treinamento da LeNet A



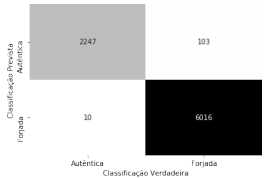
(b) Acurácia durante o treinamento da LeNet A



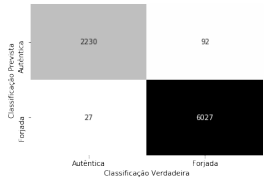
LeNet

Figura 6: Matrizes de confusão dos melhores modelos obtidos com a arquitetura LeNet.

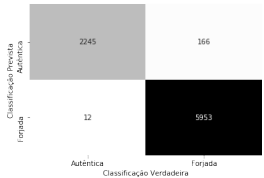
(a) LeNet A



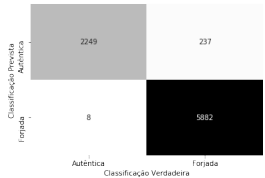
(b) LeNet B



(c) LeNet C



(d) LeNet D



AlexNet

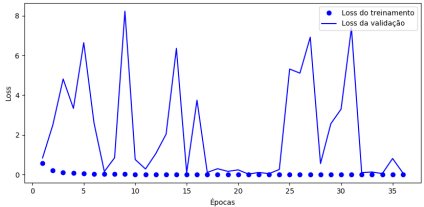
Tabela 6: Detalhamento dos melhores modelos obtidos com a arquitetura AlexNet.

Identificação	Otimizador	*Patience*	Função de Ativação	Acurácia	F-Score
AlexNet A	Adam	15	ELU	0.9654	0.9393
AlexNet B	SGD	10	*Leaky* ReLU	0.9601	0.9311
AlexNet C	SGD	5	SELU	0.9561	0.9244

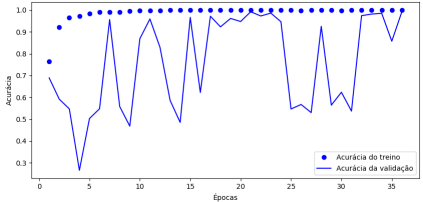
AlexNet

Figura 8: Histórico de *loss* e acurácia durante o treinamento dos melhores modelos obtidos com a arquitetura AlexNet.

(a) *Loss* durante o treinamento da AlexNet A



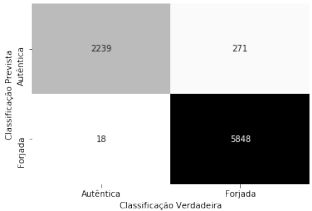
(b) Acurácia durante o treinamento da AlexNet A



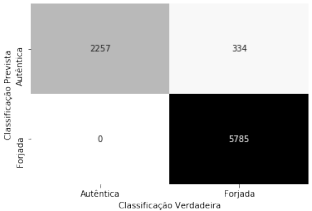
AlexNet

Figura 10: Matrizes de confusão dos melhores modelos obtidos com a arquitetura AlexNet.

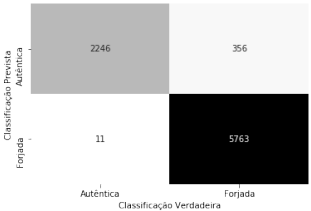
(a) AlexNet A



(b) AlexNet B



(c) AlexNet C



Agenda

1. Introdução

2. Objetivos

3. Justificativa

4. Metodologia

5. Cronograma

6. Fundamentação Teórica

7. Solução Proposta

8. Resultados Parciais

9. Considerações Finais

10. Referências

Considerações Parciais

- Total de 72 redes treinadas

Considerações Parciais

- Total de 72 redes treinadas
- Melhor desempenho: LeNet
  - **Acurácia**: 0.9755
  - ***F-Score***: 0.9865
  - **Parâmetros e Hiperparâmetros**: Otimizador RMSprop, *patience* 5 e função de ativação *Leaky* ReLU.

Considerações Parciais

- Total de 72 redes treinadas
- Melhor desempenho: LeNet
  - **Acurácia**: 0.9755
  - ***F-Score***: 0.9865
  - **Parâmetros e Hiperparâmetros**: Otimizador RMSprop, *patience* 5 e função de ativação *Leaky* ReLU.
- Próximos passos:
  - Arquiteturas com menos parâmetros (MobileNet, SqueezeNet)
  - Arquiteturas mais profundas (VGG-16, Inception)

Agenda

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