Um Estudo em Grafos Aplicados a Reconhecimento de Padrões com Foco em Biometria

Caio Vianna Rizzo [a], Mariana Ferreira Rocha [b]

[a] caiov.r@hotmail.com
[b] marianaferrocha@gmail.com
[a,b] Universidade Federal do Espírito Santo

Abstract

This paper interpret the history of graphs by considering how, why and when they have been used in pattern recognition (PR). With an overview of some different methods used in biometric recognition, and them focusing in two techniques from biometric recognition in graphs, the elastic bunch graph method, used to recognize human faces and the matching method for fingerprints. We also present an algorithm for the application of each one of them.

Keywords: Grafos, Reconhecimento de Padrões, Biometria, Reconhecimento Biométrico, Reconhecimento de Faces, Reconhecimento de Impressão Digital.

1. Introdução

Padrões estão por toda a parte no mundo virtual, podendo serem observados fisicamente ou matematicamente, com a aplicação de algoritmos desenvolvidos para reconhecê-los. Exemplos seriam as cores nas roupas, as características em comum entre os idiomas, reconhecimento biométrico de pessoas, de documentos, entre muitos outros. Portanto reconhecer um padrão pode ser definido como a classificação de dados, baseando-se em conhecimento já adquirido ou em informações extraídas, estatisticamente de padrões ou suas representações [1]. Entre esses tipos de padrões citados acima esse artigo irá se aprofundar em reconhecimento de padrões na área da biometria, que foca na identificação de padrões baseada em características fisiológicas (como rosto, impressões digitais, geometria do dedo, geometria da mão, veias da mão, palma, íris, retina, orelha e voz) e características comportamentais (como postura, assinatura e dinâmica em teclados) [2].

Reconhecimento de padrões se preocupa com a identificação de regularidades em dados, através do uso de algoritmos e com o uso dessas regularidades, realiza ações como classificar os dados em diferentes categorias [3]. Esse campo de estudos desenvolveu-se significativamente nos anos 60, sendo um assunto interdisciplinar, abrangendo desenvolvimentos nas áreas de estatística, engenharia, inteligência artificial, informática, psicologia e fisiologia, entre outros [4].

Durante os anos muitos métodos foram propostos para modelar o problema de reconhecimento de padrões como a utilização de vetores, grafos e inteligência artificial, mas este artigo tem como o objetivo focar nas soluções envolvendo grafos trazendo com maiores detalhes como é feito a modelagem do problema e os algoritmos utilizados para sua solução, com foco no reconhecimento de faces e de digitais.

2. Reconhecimento de Padrões

O estudo de reconhecimento de padrões em grafos vem sendo estudado desde a década de 70, antes desse período os estudos eram focados no reconhecimento estatístico de padrões(SPR - Statistical Pattern Recognition) para representar objetos do mundo real por meio de um conjunto de medidas, chamadas features(características). Uma vez que estas n características foram extraídas, um objeto se torna um ponto n-dimensional no espaço vetorial correspondente. Uma propriedade pode ser extraída dessas informações, sempre que pontos estivessem pertos uns dos outros no espaço vetorial significa que eles são similares no mundo real, como mostra a figura A [5] .

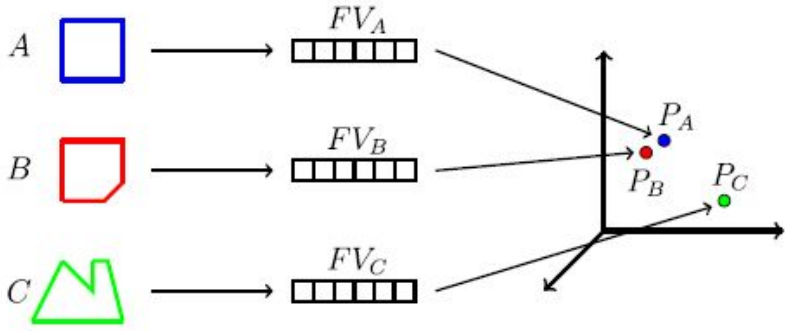

Figura A [5]

No final da década de 70 pesquisadores desta área começaram a se questionar se o uso de vetores poderia resolver todos os problemas de reconhecimento de padrões. A resposta estava relacionada ao fato que vetores de comprimento prefixado não são adequados para representarem padrões complexos, pois todos os vetores têm que preservar o mesmo comprimento, independentemente do tamanho ou complexidade dos objetos que estão sendo abstraídos. Outra limitação seria que não há possibilidade direta de descrever relações binárias que possam existir entre diferentes partes de um objeto. Então nesse período descobriram que seria muito mais apropriado o uso de grafos para representar as estruturas que descrevem os padrões, pois como o reconhecimento de padrões tem como objetivo decompor um objeto em termos de suas partes constituintes, ou seja, seus sub-padrões e como esses objetos são feitos de partes adequadamente conectadas umas às outras, grafos seriam ideal para a sua representação. Os vértices valorados podem ser usados como descritores das partes que compõem os objetos, enquanto as arestas representam a relação entre essas partes. [5][6][7].

Por essa razão muitas pesquisas foram feitas baseadas nessa ideia de solucionar o problema de reconhecimento de padrões através de diferentes representações de grafos como matching, graph edit distance (GED) e kernels de grafos. [5].

Outra forma que é muito popular no mundo acadêmico para reconhecimento de padrões são as Redes Neurais Artificiais [8]. Estas foram inspiradas pela forma em que o cérebro processa informações complexas. O cérebro processa incrementalmente as informações que recebe com o tempo e consegue com isso a habilidade de tomar decisões e mais importante neste caso, aprender conceitos e obter conclusões sobre informações complexas, cheias de ruído, irrelevantes ou parciais. Este processo é chamado de aprendizado, logo assim como um cérebro, uma rede neural pode ser treinada para solucionar diversos problemas de reconhecimento de padrões [8]. Estas técnicas são amplamente usadas,

também, no reconhecimento de faces como o survey [2] aborda, com excelentes resultados obtidos.

Este trabalho tem como foco apresentar como grafos tem sido utilizado para representar informações e auxiliar a solucionar os problemas de reconhecimento de padrões biométricos, com foco em reconhecimento facial e de impressões digitais.

2.1. Modelagem em Grafos

2.1.1 Reconhecimento Biométrico

Um sistema biométrico é em sua essência um sistema de reconhecimento de padrão, que busca identificar indivíduos com base em um vetor de características derivado de uma fisiologia específica ou comportamental. Dependendo da sua aplicação, um sistema biométrico opera, tradicionalmente, em um dos dois modos: verificação ou identificação [9]. Em modo de verificação, o sistema valida a identidade de uma pessoa, comparando as suas características biométricas capturadas com o template biométrico do indivíduo (individual's biometric template), que já foi previamente salvo no banco de dados . No modo de identificação, o sistema reconhece um indivíduo buscando pelo seu template em toda a base de dados até encontrar uma correspondência (*math*) nas informações. Realizando portanto, neste caso, uma comparação um-para-muitos para estabelecer a identidade de um indivíduo, ou falhar quando este não existir na base de dados [9].

Um sistema biométrico clássico consiste em 4 componentes básicas [10]:

1) Um módulo sensor que adquire os dados biométricos;
2) Módulo de extração de características extraction, onde os dados brutos adquiridos do sensor são processados e seu vetor de características é obtido;
3) Módulo de matching, onde os vetores são comparados com os armazenados no template;
4) Módulo de decisão, o qual é responsável pela identificação do usuário ser estabelecida ou uma requisição de identificação é aceita ou rejeitada.

A tabela 1 abaixo reúne as formas de identificação de padrões biométricos mais famosos e faz uma comparação entre eles em diversos termos.

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Tabela 1 Comparação de várias tecnologias biométricas [11].

Existem diversas aplicações comerciais para o reconhecimento biométrico, os principais podem ser divididos em 3 grupos [11]:

- Aplicações comerciais como redes de computadores, segurança de dados digitais, e-commerce, acesso a internet, cartões de crédito, controle de acesso em estabelecimentos, telefone celular, controle de dados médicos e aprendizado a distância;
- Governamentais como documentos de identidade, carteiras de habilitação, segurança social, estado do bem-estar, controle de fronteira e de passaporte;
- Aplicações forenses como identificação de corpos, investigação criminal, identificação de terroristas, de parentesco e de crianças desaparecidas.

2.2.2 Reconhecimento Facial

O reconhecimento facial é com certeza o método biométrico mais comum utilizado por humanos para fazer o reconhecimento de pessoas, portanto criar tecnologias capazes de realizar o mesmo processo é algo intuitivo. Este é um método não intrusivo e bastante útil para aplicações secretas de reconhecimento. As aplicações para reconhecimento facial variam desde estáticas, como fotos de presos, a dinâmicas, como identificação de rostos em meio a situações incontroláveis (metrôs, aeroportos). A verificação de faces envolve extração das características baseando-se em uma imagem de duas dimensões do rosto do usuário e fazendo um *matching* com o template guardado no banco de dados [10].

As abordagens mais populares para reconhecimento facial são baseadas em [10]:

1) A localização e tamanho dos atributos faciais, como olhos, sobrancelhas, nariz, lábios e queixo, e suas relações espaciais;

2) A análise global da imagem da face, a qual representa o rosto como uma combinação de pesos ponderados de um número de faces canônicas.

Esses sistemas têm dificuldade em reconhecer um rosto de imagens capturadas de ângulos diferentes ou sobre condições de iluminação diferentes. Sistemas deste tipo devem ser capazes de identificar automaticamente uma face em uma imagem, extrair suas características e então reconhecer o rosto de uma pessoa de qualquer posição, sendo um agravante de dificuldade o fato desta ser um órgão que muda com o tempo e possui uma grande variedade de expressões [10]. Portanto esta não é uma tarefa simples, mas já é realizada nos dias de hoje pelos gigantes da internet como o Facebook, Amazon e Google.

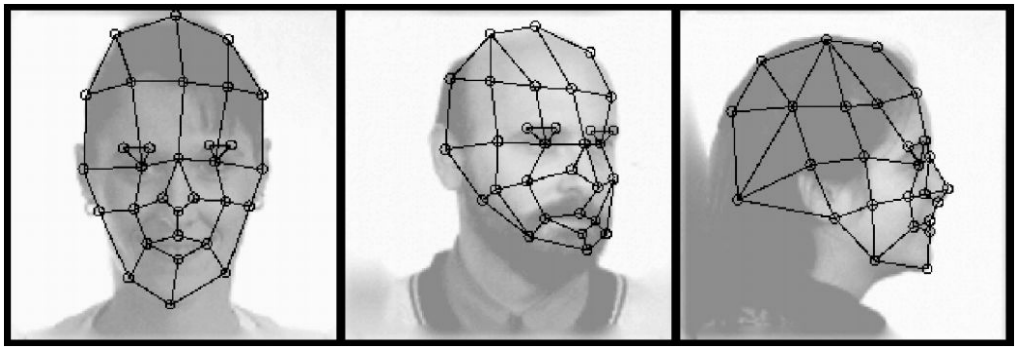

Figura B. Grid de grafo adaptado para diferentes poses [12].

Um método bem conhecido, baseado em *features* é o chamado *Elastic Bunch Graph Matching*, proposto por Wiskott et al. [12]. Esta técnica é baseada no *Dynamic Link Structures* [13]. Um grafo para um rosto específico é gerado como segue: um conjunto de pontos fiduciais sobre a face são escolhidos (Figura B). Cada um destes pontos se torna um vértice em um grafo conexo e é rotulado com as respostas do filtro de Gabor [14] aplicado em uma janela ao redor do ponto fiducial. Cada aresta é rotulada com a distâncias entre os pontos fiduciais correspondentes. Um conjunto representativo destes grafos é combinado em uma estrutura de pilha, chamada "*face bunch graph*" (Figura C). Uma vez que o sistema possui este *face bunch graph*, grafos para novos rostos podem ser gerados automaticamente pelo *Elastic Bunch Graph Matching*. O reconhecimento de uma nova imagem de rosto é então feita pela comparação do grafo desta imagem com todas as faces conhecidas e escolhendo aquela com o maior valor de similaridade. Desta forma, uma taxa de reconhecimento de até 98% pode ser alcançada para o primeiro *rank* e 99% para os primeiros 10 *ranks* usando uma galeria de 250 indivíduos [2] [12].

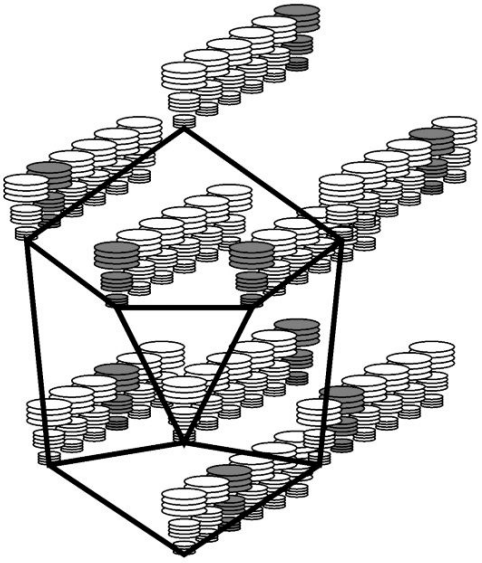

Figura C. *Face Bunch Graph* (FBG) [12]

O algoritmo para reconhecimento de faces, para uma única pose, pode funcionar como segue abaixo [14]:

Passo 1: Construindo o grafo da face. O primeiro passo para inicializar o sistema é definir o grafo para a pose dada. Então com a primeira imagem, manualmente definimos as localizações dos vértices no rosto, os quais serão fáceis de localizar, como os cantos dos olhos ou da boca, o centro dos olhos, a ponta do nariz, alguns pontos no contorno, etc. Também definimos as arestas entre os vértices. Este constitui o primeiro grafo de face.

Passo 2 Construindo um *face bunch graph*. O único grafo de rosto definido acima pode ser visto como um *bunch graph* que possui apenas uma instância. podendo ser combinado com uma segunda imagem de rosto, mas se as primeiras 2 imagens não forem parecidas o suficiente, o *match* é de baixa qualidade. Depois de algumas correções manuais, como irregularidade na demarcação do queixo e nariz, esta segunda instância está pronta para ser integrada ao *bunch graph*. Então este *bunch graph* é combinado com uma terceira imagem, com mais alguns ajustes manuais. E com a repetição deste processo o *bunch graph* cresce e conforme seu crescimento ocorre, menos ajustes são necessários a cada nova imagem combinada, tornando portanto o *match* mais e mais confiável. Assim que obtemos uma qualidade boa de *match*, que requer o mínimo de ajustes, podemos parar este processo e o *bunch graph* estará pronto. Neste exemplo podemos assumir que 100 imagens foram usadas para construir este grafo e obter uma boa qualidade de *match*.

Passo 3: Construindo a galeria de modelos de grafos. Uma vez que agora temos um *bunch graph* que provê uma boa qualidade em encontrar as localizações dos vértices em um novo rosto, podemos processar as imagens automaticamente. Neste exemplo, as demais 900 imagens restantes.

Passo 4: Construindo o *probe graph*. Uma nova imagem é passada e para encontrar esta pessoa representada na galeria, primeiramente deve-se criar o grafo para esta imagem de rosto, por um processo exatamente igual para o feito para as imagens usadas para a criação do modelo.

Passo 5: Comparação com todos os grafos do modelo. O grafo da imagem é comparada com todos os modelos de grafo, tendo n resultados de semelhança de acordo com o número de grafos que foram salvos, neste exemplo 1000 valores. Este processo constitui a

base para a tomada de decisão, comparando os grafos somente com a função de semelhança que pode ser vista em [14].

Passo 6: Reconhecimento. Para o reconhecimento é claro que o modelo de grafo com maior similaridade com o grafo da imagem passada é o melhor candidato para a fase de reconhecimento. Porém, se a maior valor de semelhança é relativamente pequeno, o sistema pode decidir que esta nova imagem de rosto não pertence a ninguém da galeria de modelos de grafo salvos, se houver mais de um grafo com valor alto de similaridade, o sistema pode decidir que a pessoa é uma das que estão na galeria, mas existem vários candidatos possíveis. Apenas se o maior valor de igualdade é alto e razoavelmente maior que os demais, o sistema pode de fato reconhecer de que pessoa na galera aquela imagem é com uma boa precisão.

Este sistema atingiu 98% de reconhecimento em uma galeria de 250 imagens frontais de rosto, 57% em imagens de semi-perfil e 84% em perfil [12].

2.2.3 Reconhecimento de Impressão Digital

O uso de digitais para o processo de identificação de pessoas tem sido utilizada a muito tempo desde o antigo Egito sendo utilizada para identificar criminosos e para registrar transações comerciais [15] e até os tempos atuais projetar algoritmos para extrair características importantes de impressões digitais e combiná-los ainda é um problema desafiador e importante no reconhecimento de padrões [16].

O processo de identificação por digital é baseado em encontrar padrões nas papilas (elevações da pele) da superfície do dedo. As impressões digitais tem três características fundamentais que explica o porque esse processo tem sido muito utilizado durante os anos, que é o fato de não existir impressões digitais semelhantes no mundo, delas serem imutáveis e por isso são uma das características únicas em sistemas de identificação [17]. A maior dificuldade nesse processo se deve a grande variabilidade intra-classe e à grande semelhança entre classes nos padrões de impressões digitais [16].

Uma digital consiste em linhas de papilas que geralmente se estendem de forma paralela e os pontos onde essas linhas interceptam ou se terminam são chamadas de minúcias. Outra característica das impressões digitais que determinam singularidades ou regiões singulares são as áreas denominadas core e delta que representam os fluxos de linhas de papilas e são frequentemente utilizadas na classificação de impressões digitais, como mostra a figura D [17].

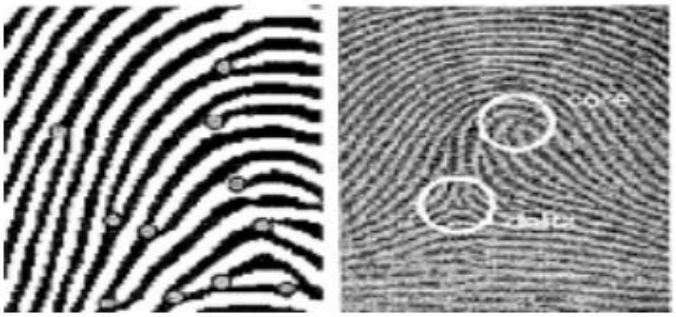

Figura D - Na esquerda estão as minúcias e na direita as áreas delta e core [17].

Neste trabalho, vamos focar na codificação das impressões digitais em formato de grafos para fazer essa associação se usa o algoritmo abaixo[18]:

Algoritmo 1: Associação de um grafo valorado e colorido a uma impressão digital

Passo 1: Identificar todas as características singulares da digital, ou seja, as minúcias, cores e deltas na impressão digital.

Passo 2: Associe um vértice a cada uma das características da papilas encontradas na Etapa. Use cores diferentes para identificar cada tipos de característica (por exemplo: verde para as minúcias no caso de bifurcação, vermelho no caso de minúcias de término, amarelo para os cores e azul para deltas).

Passo 3: Construa uma aresta entre cada dois vértices que estão em um fluxo conectado de papilas.

Passo 4: Associe um peso a cada aresta que representa o seu comprimento medido em centímetros.

Passo 5: Associe para cada vértice, encontrado no passo 2 um par de números (m, n), onde, m corresponde a um caractere que representa a característica da papilas e o n corresponde ao grau do vértice.

Para melhor compreensão do funcionamento do algoritmo a figura E demonstra seu funcionamento.

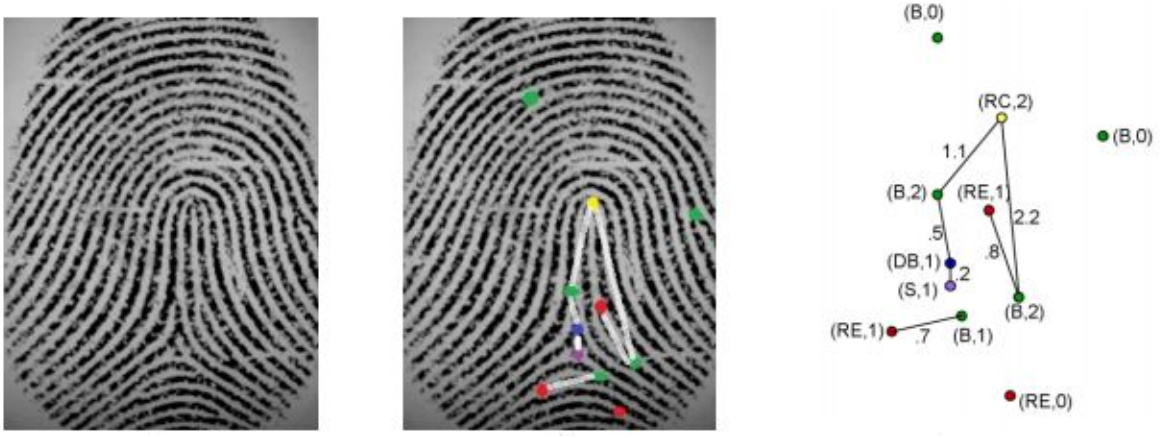

Figura E [18]

Para poder reconhecer se duas impressões digitais são iguais, ambas modeladas pelo algoritmo acima, é necessário a execução de mais dois algoritmos uma para classificar cada impressão digital usando três níveis de classificação e outro para conferir se existe um matching entre os dois grafos [18].

Algoritmo 2: Classificação da impressão digital

Passo 1: Determine se a impressão digital tem um core. Se sim, vá para o Passo 3. Se não, vá para o Passo 2.

Passo 2: Classifique a impressão digital como Plain Arch (PA), sem core e sem delta, e vá para a Passo 5.

Passo 3: Determine se a impressão digital tem um delta. Se sim, vá para a Passo 5. Caso contrário, vá para a Passo 4.

Passo 4: Classifique a impressão digital como Tented Arch (TA), com core mas sem delta, e vá para a Passo 8.

Passo 5: Determine o número de deltas. Se tiver apenas um delta, vá para o Passo 6. Se tiver mais de dois vá para a o Passo 7.

Passo 6: Classifique a impressão digital como Radial Loop (RL), quando a inclinação do delta é para o lado do nervo radial (polegar) da mão, ou Ulnar Loop (UL), quando a inclinação do delta é para o lado do nervo ulnar (dedo mindinho) da mão, e vá para a Passo 8.

Passo 7: Classifique a impressão digital como Plain Whorl (PW), Pocket Whorls (CPW), Double Loop Whorl (DLW) ou Whorls Acidentais (AW)) e vá para a Passo 8.

Passo 8: Conte o número de diferentes características das papilas existem (A quantidade de cores diferentes foram usadas para colorir o grafo).

Passo 9: Classificação Nível Um: Classifica a impressão digital (Pattern Type (PT), Sub-Pattern Type (SPT), # of Ridge Characteristics (RC)), onde PT pode ser Arch (A), Loop (L), or Whorls (W).

Passo 10: Conte o número de componentes conexas(CC), número total de vértices (V) e número total de arestas (E), do grafo.

Passo 11: Classificação de Nível Dois: Classifica a impressão digital como (CC, V, E).

Passo 12: Encontre as características das papilas para cada vértice do grafo(m_i , i = 1, 2, …).

Passo 13: Encontre o grau de cada vértice (n_i , i = 1, 2, …) e o peso de cada aresta adjacente (R_i , i = 1, 2, …) do grafo.

Passo 14: Classificação de Nível Três: Classifica cada vértice no grafo como (m_i , n_i , $R_1 \ldots R_n$).

Para compreender melhor algumas classificações usadas no algoritmo acimo segue a Figura F com mais detalhes.

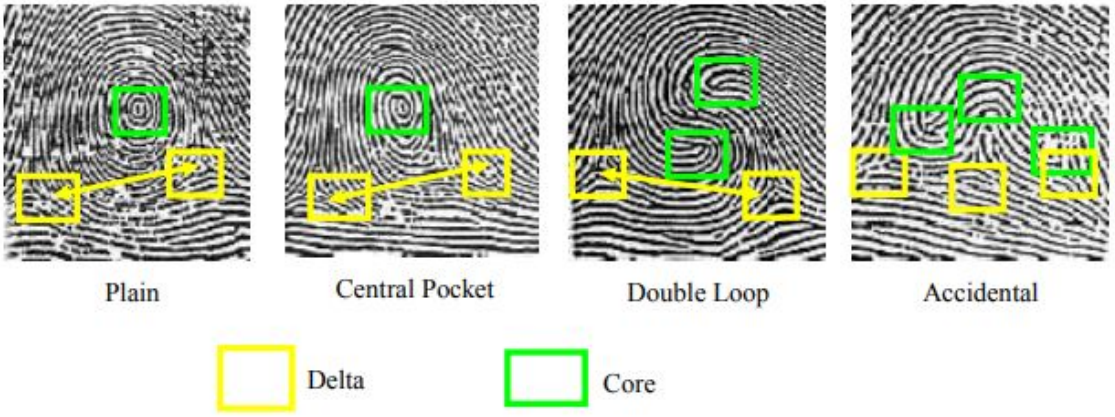

Figura F - classificação dos Whorls (Espirais) [18]

O algoritmo determina se dois grafos são isomorfos, ou seja, se eles podem ser combinados de forma que todas as suas características sejam idênticas e, sendo assim, os dois grafos são considerados isomórficos [18].

Algoritmo 3: Verifica se dois Grafos são iguais

Entrada: Dois grafos classificados pelo Algoritmo 2.

Passo 1: Confere se a classificação do primeiro nível dos dois grafos são iguais, caso contrário os grafos são diferentes encerra o algoritmo.

Passo 2: Confere se a classificação do segundo dos dois grafos são iguais, caso contrário os grafos são diferentes encerra o algoritmo.

Passo 3: Confere se a classificação do terceiro dos dois grafos são iguais, caso seja verdade as impressões digitais são correspondentes, caso contrário os grafos são diferentes.

3. Conclusão

Com este trabalho podemos perceber que os grafos já foram uma excelente alternativa para reconhecimento de padrões, com boas taxas de reconhecimento (98%). Porém nos últimos anos tem perdido muito espaço no meio acadêmico e comercial para as redes neurais artificiais, que conseguem atingir taxas tão expressivas quanto, e principalmente quando se trata de reconhecimento facial, possuem muito mais flexibilidade para diferentes poses e ambientes. O que pode ser mostrado pelo uso dessas tecnologias pelas grandes empresas da internet como Facebook e Google, conseguindo identificar pessoas sob as mais diversas condições remotas de ambiente e posicionamento.

Referências:

[1] PATTERN Recognition Introduction. 2018. Disponível em: <https://www.geeksforgeeks.org/pattern-recognition-introduction/>. Acesso em: 02 dez. 2018.

[2] R. Jafri, H. R. Arabnia. “A Survey of Face Recognition Techniques”. Journal of Information Processing Systems, June 2009,. Vol.5, No.2, p. 41-68.

[3] C. Bishop,. Pattern Recognition and Machine Learning. Cambridge, U.K: Springer, 2006. p 738.

[4] A. K. Jain, R. Bolle, and S. Pankanti, "Biometrics: Personal Identification in Networked Security," A. K. Jain, R. Bolle, and S. Pankanti, Eds.: Kluwer Academic Publishers, 1999.

[5] M. Vento, “A long trip in the charming world of graphs for Pattern Recognition.” Pattern Recognition, vol. 48, p. 291-301, 2015.

[6] H. Bunke, K. Riesen. "Recent advances in graph-based pattern recognition with applications in document analysis." Pattern Recognition Vol. 44, n. 5, p. 1057-1067, 2011.

[7] P. Foggia, G. Percannella, M. Vento. "Graph matching and learning in pattern recognition in the last 10 years." International Journal of Pattern Recognition and Artificial Intelligence, vol. 28, n. 01, p. 1450001, 2014.

[8] Samarasinghe, S. (2007). Neural Networks for Applied Sciences and Engineering. New York: Auerbach Publications.

[9] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy, pp. 33-42, March/April 2003.

[10] K. Delac, M. Grgic. "A survey of biometric recognition methods." 46th International Symposium Electronics in Marine. Vol. 46, p. 16-18, 2004.

[11] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-19, January 2004.

[12] L. Wiskott, J.-M. Fellous, N. Krüger, and C. von der Malsburg, "Face Recognition by Elastic Bunch Graph Matching," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.19, pp.775-779, 1997.

[13] M. Lades, J. C. Vorbrüggen, J. Buhmann, J. Lange, C. v. d. Malsburg, R. P. Würtz, and W. Konen, "Distortion invariant object recognition in the dynamic link architecture," IEEE Trans. Computers, Vol.42, pp.300-311, 1993.

[14] L. Wiskott, R. P. Würtz, G. Westphal, Elastic Bunch Graph Matching. Scholarpedia, 2014 Disponível em: <http://www.scholarpedia.org/article/Elastic_Bunch_Graph_Matching>. Acesso em: 02 dez. 2018.

[15] D. K. Isenor, G. Z. Safwat. "Fingerprint identification using graph matching." Pattern Recognition, vol. 19, n. 2, p. 113-122, 1986.
[16] S. Dyre, C.P. Sumathi, “A Survey on Various Approaches to Fingerprint Matching for Personal Verification and Identification”, International Journal of Computer Science & Engineering Survey, Vol.7, No.4, August 2016.
[17] M. Tarjoman, Z. Shaghayegh. "Automatic fingerprint classification using graph theory." Proceedings of World Academy of Science, Engineering and Technology. Vol. 30, p. 831-835, 2008.
[18] M. A. Karim, V. Vasilevska, “Having Fun with Graph Theory and Forensics”, A CCICADA Homeland Security Module, 2015.