Interoperabilidade de Assinaturas Keystroke Para Uso em Sistemas de Segurança Baseados em Login e Senha : Uma Análise de Características Temporais

Ana Beatriz da C. Figueiredo[1], **Rodolfo B. de B. Garcia**[1]

[1]Departamento de Computação (DCOMP) – Universidade Federal de Sergipe (UFS)
Av. Marechal Rondon, – Jardim Rosa Elze – CEP 49100-000
São Cristóvão – SE – Brazil

abeatrizcf@academico.ufs.br, rodolfo.botto@dcomp.ufs.br

Abstract. *Due to the increasing use of mobile phones at the expense of computers and notebooks, coupled with the absence of built-in sensors in these devices, the interoperability of passwords using keystroke dynamics on these two types of keyboards becomes relevant. For this analysis, a quantitative methodology with experimental elements was used, employing the extraction of mathematical and graphical data in addition to classification methods. Consequently, the results demonstrate that the interval behaviors of the touchscreen dataset are in line with previously proven scientific results. Therefore, it is suggested that interoperability between the two types of keyboards is possible, but with an interval equalization process.*

Resumo. *Em decorrência do crescente aumento do uso de celulares em detrimento do uso de computadores e notebooks atrelado a ausência de sensores de fábricas nestes dispositivos, a interoperabilidade entre senhas fazendo uso do keystroke nesses dois tipos de teclado faz-se relevante. Para tal análise, empregou-se uma metodologia quantitativa com elementos experimentais através da extração de dados matemáticos e gráficos além de métodos de classificação. Dessa forma, os resultados demonstram que os comportamentos dos intervalos da base touchscreen estão em consonância com resultados científicos previamente comprovados. Sendo assim, indica-se que é possível a interoperabilidade dos dois tipos de teclado, mas com um processo de equalização de intervalos.*

1. Introdução

A crescente demanda por métodos de autentificação cada vez mais seguros e eficazes em dispositivos como smartphones e computadores pessoais traz consigo uma gradual adesão a assinaturas biométricas. Ratificando essa afirmativa, é válido mencionar a pesquisa da Juniper Research de 2022, que projeta um aumento de 383% no volume de pagamentos móveis remotos autenticados biometricamente até 2027 [TI Inside 2024]. É válido ressaltar que dispositivos móveis como o celular, por exemplo, detêm diversos sensores que permitem a aplicação de uma grande diversidade de assinaturas biométricas, tanto fisiológicas (a impressão digital, o reconhecimento facial ou de voz) quanto comportamental (keystroke). Já os desktops e notebooks não possuem essa variedade de sensores vindos de fábrica, necessitanto da aquisição de ferramentas específicas para tais meios de

autenticação. Uma forma de biometria acessível financeiramente para esses dispositivos é o Keystroke, que não necessita de um hardware específico e identifica usuários a partir da dinâmica de digitação obtida por um teclado físico tradicional ou touchscreen.

A partir da perspectiva exposta, faz-se necessária a observação da realidade na qual constata-se que a utilização de dispositivos móveis cresceu exponencialmente nos últimos anos. Em contrapartida, o uso de computadores sofre uma queda gradativa. Em consonância com essa afirmativa, estão os resultados da Pnad Contínua sobre Tecnologia da Informação e Comunicação de 2022 realizada pelo IBGE [Folha de S.Paulo 2023]. Na pesquisa em questão, constatou-se que o aparelho celular é o equipamento mais usado para o acesso à internet no Brasil. Conforme o órgão, 98,9% dos usuários de internet, ou seja, pessoas a partir de dez anos que nos três meses antecedentes a pesquisa acessaram pelo menos uma vez a rede, utilizaram como meio para tal ação, aparelhos celulares. Dado este que reflete um crescente aumento do uso de dispositivos móveis previamente referido considerando que a mesma informação estatística foi de 98,8% e 94,8% para os anos de 2021 e 2016, respectivamente. Por outro lado, o computador foi usado por 35,5% dos usuários em 2022 ou 57,4 milhões do total de 161,6 milhões. Analisando o quantitativo de anos precedentes, nota-se uma paulatina queda nesses valores, já que o percentual relativo aos computadores era de 41,9% em 2021 e 63,2% em 2016.

Além disso, já é de conhecimento que as assinaturas keystroke são esquecidas quando não usadas e necessitam de atualização constante para manter-se estáveis [Montalvão et al. 2015]. A baixa periodicidade e repetição de assinaturas keystroke em dispositivos como desktops e notebooks podem dificultar o exercício e a utilização do mesmo em teclados físicos, já que essa assinatura biométrica exige do usuário uma padronização da maneira como ele digita. Por outro lado, pode-se chegar a conclusão que as pessoas digitalmente ativas apresentam uma frequência significativamente maior de digitação nos seus respectivos dispositivos móveis se comparada ao uso de desktops e notebooks, por exemplo.

Nesse sentido, o contexto supracitado exerce maior influência em sistemas de segurança e suas formas de autentificação, principalmente em dispositivos fixos. Por conta disso, este trabalho levanta a hipótese de que, se dispositivos móveis são usados de forma tão ampla e a assinatura por keystroke pode ser constantemente atualizada durante seu envelhecimento, então é possível usar a forma da assinatura obtida por dispositivos móveis para validar assinaturas biométricas esporadicamente introduzidas em dispositivos não móveis.

Assim sendo, objetiva-se por meio deste trabalho analisar as características temporais de assinaturas keystroke obtidas por teclados de tipos distintos (touchscreen e físico) e verificar a possibilidade futura de interoperabilidade de métodos de reconhecimento biométrico em diferentes dispositivos (móveis e fixos), considerando uma única assinatura keystroke, ligada ao contexto de segurança baseado em login e senha.

Dessa forma, de acordo com experimentos aqui descritos, há indícios fortes de que essa interoperabilidade seja possível, pois algumas características observadas nas assinaturas compartilham semelhanças, o que motiva a realização dos trabalhos futuros propostos no fim deste artigo.

Diante disso, a estrutura desse artigo apresenta-se da seguinte forma: na Seção

2, são exibidos os principais conceitos teóricos sobre assinaturas keystroke; a Seção 3 descreve a metodologia empregada na aplicação desses conceitos; em seguida, na Seção 4, é detalhado o processo de experimentação e discussão para avaliar uma possível interoperabilidade entre assinaturas keystroke; e, por fim, são listadas as conclusões parciais na Seção 5 e os trabalhos futuros na Seção 6.

2. Fundamentação Teórica

As inovações tecnológicas no âmbito de segurança acarretaram grande ênfase no conceito de assinaturas biométricas. Estas consistem em formas de autenticação digital baseadas em informações relacionadas aos atributos fisiológicos ou comportamentais de uma pessoa. Diante disso, existem dois tipos de assinaturas biométricas: as fisiológicas, ou seja, baseadas em características físicas envolvendo a impressão digital, a íris e o rosto [Habeeb 2019] e as comportamentais, isto é, que se refere a qualquer característica capaz de identificar um indivíduo por meio do seu comportamento, como padrões de caminhada e o método explorado no presente artigo, o keystroke [Stragapede et al. 2023].

O keystroke dynamics consiste na análise do padrão de digitação de uma pessoa. Dessa forma, essa técnica utiliza as características únicas apresentadas pelos indivíduos ao desempenharem o processo de digitação, seja em teclados físicos ou teclados touchscreen. A partir de dados temporais coletados durante a digitação, algoritmos criam modelos e reconhecem o comportamento capaz de identificar a pessoa que está digitando. De tal forma, essa biometria surge como uma ferramenta importante para a cibersegurança, pois promete ser não intrusiva e ser economicamente viável. Além disso, não requer hardware adicional, o que facilita sua implementação também em desktops e notebooks [Shadman et al. 2023].

Dentro dessa esfera, conceitos importantes sobre os dados temporais são levantados e mostrados na Figura 1. O primeiro parâmetro relevante é o intervalo “Holding” (H), que consiste no tempo que uma tecla permanece pressionada. Outro conceito é o intervalo “DownDown” (DD), que consiste no intervalo entre o pressionamento de uma tecla e o pressionamento da tecla seguinte. Por fim, tem-se o intervalo “Updown”(UD), que abrange o momento em que uma tecla é liberada até o momento no qual a próxima tecla é pressionada.

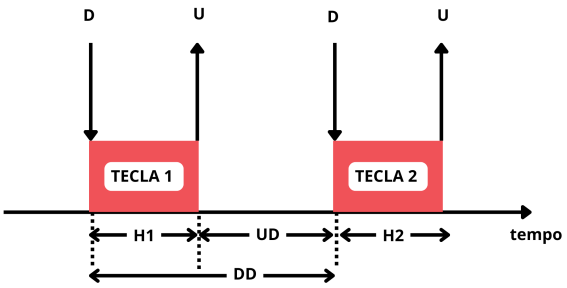

Figura 1. Representação dos intervalos (baseada em [Xiaofeng et al. 2019])

Ademais, trabalhos prévios identificaram padrões de comportamentos em

assinaturas keystroke obtidas em teclados físicos, que serão experimentados aqui servindo-se agora de assinaturas provenientes de teclados touchscreen.Em [Montalvão Filho and Freire 2006] foi constatado que os intervalos DD têm forma de distribuição log-normal e, com um método de equalização proposto pelos autores, que é possível realizar a identificação dos usuários. Em [Montalvão et al. 2015] foi explicitado que os intervalos H também se distribuem em forma log-normal e os intervalos UD são considerados redundantes, sendo assim retirados das análises. Por fim, o trabalho de 2015 também identificou os processos de estabilização e esquecimento das assinaturas tendo em vista que após uma sequência de repetições foi notado que as primeiras assinaturas de cada sessão foram as mais instáveis.

3. Metodologia

O presente artigo consiste em uma pesquisa cuja metodologia abordada foi uma análise quantitativa com elementos experimentais ligados a caracterização de assinaturas biométricas baseadas na técnica do keystroke obtidas por teclados físicos e touchscreen. Para tal abordagem, as etapas realizadas são as subsequentes: obtenção das bases de dados, pré-processamento de dados, classificação das assinaturas keystroke e extração de características das mesmas.

Para a etapa de extração das características foi utilizada a linguagem de programação Python e sua respectiva biblioteca pandas. Além desta, a fim de proceder cálculos matemáticos e obtenção de gráficos, como histogramas e curvas gaussianas, as bibliotecas matplotlib e numpy foram aplicadas. Destarte, também empregou-se o uso de um algoritmo de aprendizado de máquina supervisionado de classificação, o K-Nearest Neighbors (KNN), a fim de gerar e interpretar as acurácias do processo de distinção entre as amostras obtidas por teclados de diferentes tipos.

3.1. Obtenção das bases de dados

Neste trabalho foram selecionados dois datasets com registros de assinaturas keystrokes, compostas por intervalos H, DD e UD, sendo um dataset obtido por teclado físico (Base F) [Killourhy and Maxion 2009] e outro por teclado touchscreen (Base T) [Antal et al. 2015]. A motivação pela escolha de tais bases se deu pelo fato de adotarem a mesma palavra chave ”.tie5Roanl”. Por outro lado, faz-se necessário mencionar que as amostras das duas bases não foram obtidas pelas mesmas pessoas e, por isso, o estudo foi limitado ao comportamento geral das características sem relacionar com os autores das assinaturas biométricas. Com isso, a tarefa futura de identificação de usuários vai depender da coleta de assinaturas usando o mesmo conjunto de participantes para os dois tipos de teclados.

Nas configurações das bases originais, a Base F é formada por 31 eventos temporais no total, tem 51 participantes com 400 amostras cada um, divididas em 8 sessões com 50 assinaturas cada. Já a Base T é composta por 41 eventos temporais no total, com 42 participantes válidos (37 de tablet e 5 de smartphone), com 51 amostras por pessoa, divididas em duas sessões, porém essa divisão não é elucidada na documentação da base em questão.

3.2. Pré-processamento de dados

Após a seleção das bases que serão objetos da pesquisa, foi observado que, apesar de se tratar da mesma palavra chave, a forma como ela é digitada em teclados físicos é diferente da forma como ela é digitada em teclados touchscreens. Por isso, realizou-se o pré-processamento desses datasets, a fim de homogeneizá-los e mantê-los com o mesmo conjunto de características. Além disso, utilizou-se a mesma sequência de eventos ocorridos e a unidade de tempo padronizada em segundos.

Dando continuidade, como o método para digitar números e caracteres maiúsculos divergem no teclado físico e no touchscreen, realizou-se uma supressão das informações referentes aos caracteres “5” e “R”. Por fim, ambas as bases foram compostas pela seguinte sequência de 20 eventos juntamente com o seu identificador: user_id, H.period, DD.period, UD.period.t, H.t, DD.t.i, UD.t.i, H.i, DD.i.e, UD.i.e, H.e, H.o, DD.o.a, UD.o.a, H.a, DD.a.n, UD.a.n, H.n, DD.n.l, UD.n.l e H.l. Eventos H são os intervalos ”Holding”(por exemplo H.t representa o tempo de holding da letra ”t”), eventos DD são os intervalos ”Down Down”(DD.o.a sendo o intervalo DD entre a letra ”o”e a letra ”a”) e os eventos UD são os intervalos ”Up Down”(UD.o.a sendo o intervalo entre o UD da tecla ”o”e a tecla ”a”).

3.3. Obtenção das médias e desvios padrões

Com as bases contendo o mesmo conjunto de eventos e organizadas com a mesma sequência, realizou-se o Experimento 1 a fim de descobrir o comportamento geral das características através do cálculo das médias e desvios padrões de cada característica do conjunto de assinaturas para os 51 participantes da Base F e para os 42 da Base T.

3.4. Elaboração de histogramas e curvas gaussianas

Ainda sobre o processo de extração das características das assinaturas keystroke, realizou-se o Experimento 2, a fim de verificar se estas têm comportamentos dentro dos padrões já conhecidos na literatura científica.

Para tal, foram elaborados histogramas analisando os intervalos DD e H. O gráfico em barras representa a distribuição real dos dados de forma discreta ao passo que divide os intervalos em agrupamentos e contabiliza quantos dados são expressos em cada um dos grupos, atingindo assim o valor da frequência de cada evento para os grupos estabelecidos. Para esta elaboração foram utilizadas 1000 grupos de intervalos (bins = 1000). Além disso, esses intervalos DD e H foram distribuídos em uma Gaussiana. Para isso, cada intervalo X foi representado com sua posição na curva Gaussiana, a partir da Função Densidade de Probabilidade (PDF), $Y = log_e(X)$.

3.5. Aplicação do KNN

Como processo subsequente, através da biblioteca sklearn da linguagem python, o Experimento 3 fez uso do algoritmo K-Nearest Neighbors como método para classificar as amostras das bases F e T. O principal objetivo da aplicação do KNN nesta etapa é medir o nível de confusão que o classificador apresentará, ou seja, altas acurácias indicam que as amostras de bases diferentes não se misturam e, logo, não compartilham padrões semelhantes que possam possibilitar uma futura interoperabilidade. Para tal, este experimento aplicou a média das amostras consideradas estáveis,isto é, nas médias dos intervalos das assinaturas referentes à segunda metade de cada sessão, como comprovado por

[Montalvão et al. 2015]. Portanto, a base final foi definida com 51 participantes, cada um com 200 amostras da base F (25 amostras para cada uma das 8 sessões), acrescida das 51 amostras de cada um dos 42 participantes da base T já que a delimitação das sessões não foi determinada.

Por fim, o KNN foi executado 10 vezes e cada iteração aplicou 80% das amostras para a etapa de treino e 20% de teste. Além disso, o número de vizinhos para execução do algoritmo foi definido como 3.

4. Resultados e discussões

Nas subseções a seguir serão exibidos os resultados oriundos dos três experimentos concretizados e levantadas as discussões acerca destes.

4.1. Experimento 1: médias e desvios padrão

A partir dos dados previamente coletados e pré-processados, as médias e os desvios padrões dos intervalos DD, UD e H de todos os participantes são calculados para ambos os teclados. As Figuras 2 e 3 indicam nas curvas vermelhas os resultados para a Base F e nas curvas azuis os resultados para a Base T.

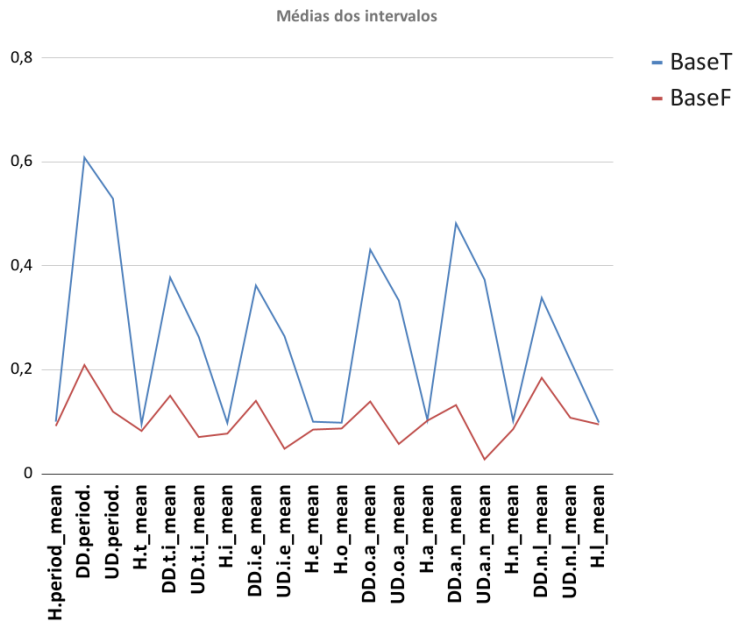

Figura 2. Gráfico das médias dos intervalos

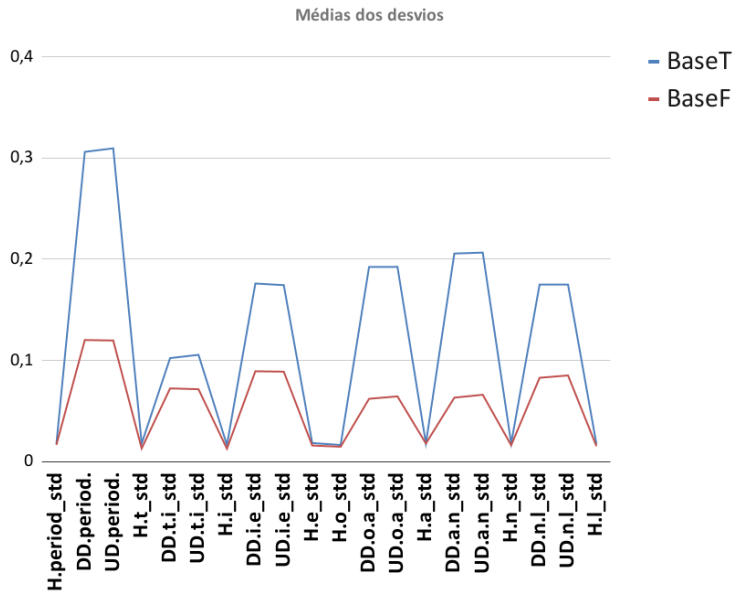

Figura 3. Gráfico das médias dos desvios padrões dos intervalos

A partir da observação empírica, nota-se que os intervalos H têm médias de intervalos e médias de desvios padrões muito próximas para os dois tipos de teclados. Isso é indicativo de que assinaturas keystroke usando eventos H podem ter comportamentos parecidos.

Para os eventos DD e UD, ambas as médias da Base F são muito menores que da Base T. Por outro lado, é possível notar algumas semelhanças, como: os valores para o evento DD.period.t (intervalo DD entre os caracteres '.' e 't') são altos para média de intervalo e de desvio padrão; demais eventos têm médias de desvio padrão mais baixos; os valores dos eventos DD são maiores que os valores dos eventos H e eventos UD não se comportam da mesma forma que os eventos DD.

Por fim, é observado que eventos DD têm padrão de comportamento semelhante e que a acentuada diferença entre os valores pode ser amenizada por uma equalização dos intervalos. Os intervalos UD não tiveram padrão de comportamento semelhante nas figuras, o que motiva o seu descarte nos próximos experimentos. Logo, as análises a partir de então incluirão 6 dados referentes aos eventos DD e 8 dados referentes aos eventos H.

4.2. Experimento 2: gaussianas e histogramas

É sabido através de [Montalvão Filho and Freire 2006] que o conjunto dos intervalos DD de todas as amostras de assinaturas keystroke obtidas por teclados físicos se distribuem de forma log-normal e, em [Montalvão et al. 2015], é comprovado o mesmo para os intervalos H.

Assim sendo, o Experimento 2, exibe as distribuições dos intervalos DD e H para as amostras da Base T. Como pode ser visto nas Figuras 4 e 5, ambos os intervalos também são distribuídos de uma forma próxima a log-normal em teclados touchscreen.

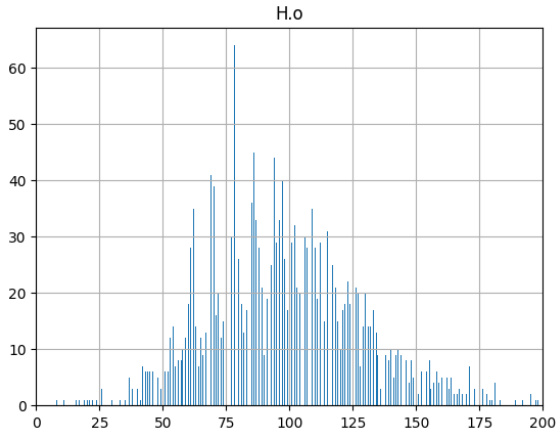

Figura 4. Histograma do intervalo H para base T

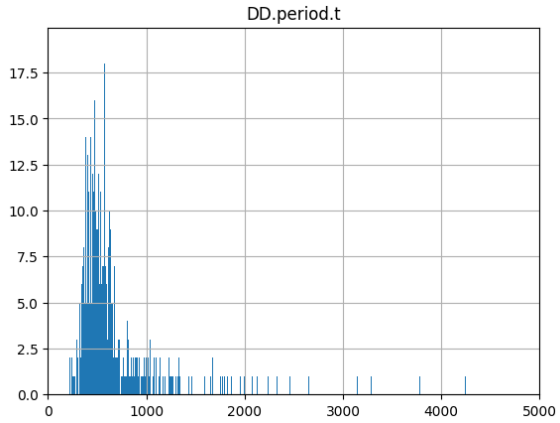

Figura 5. Histograma do intervalo DD para base T

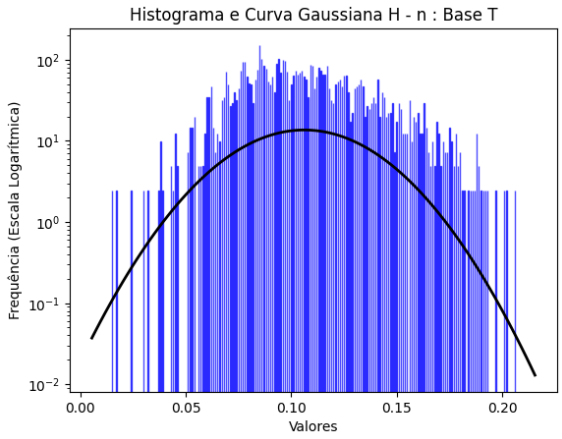

Figura 6. Gaussiana intervalo H para base T

4.3. Experimento 3 : KNN

O KNN foi executado 10 vezes para três versões de bases: usando os eventos DD e H, usando somente os eventos DD e usando somente os eventos H. Após essas execuções,

foi possível incutir que os resultados para os intervalos DD + H variaram entre 89.47% (2 vezes), 94,74% (7 vezes) e 100% (1 vez). Já para os intervalos DD sozinhos, os valores percebidos foram 89,47% (1 vez), 94,74% (7 vezes) e 100% (2 vezes). Por fim, para os intervalos H sozinhos os percentuais descritos foram 63,16% (2 vezes), 68,43% (2 vezes), 73,68% (1 vez), 78,95% (4 vezes) e 89,47% (1 vez).

Tabela 1. Média das acurácias encontradas após 10 execuções do KNN

Intervalo	Média das acurácias
DD + H	94,19%
DD	95,24%
H	74,11%

Portanto, observa-se que os valores quando analisa-se DD + H e somente DD são muito semelhantes. Adicionalmente, a análise somente com os intervalos DD apresentaram melhor acurácia que os outros dois casos analisados. Isso reflete exatamente as médias distantes obtidas entre as duas bases, o que facilita a distinção e não satisfaz a condição de futura interoperabilidade.

Também é possível constatar que as acurácias correspondentes unicamente ao intervalo H são mais baixas que os outros dois casos. Por conta das médias próximas entre as duas bases, o nível de confusão do KNN foi maior, indicando que as assinaturas keystroke usando somente os intervalos H podem ser obtidas de forma parecidas em teclados de tipos distintos, gerando indícios da possibilidade de uma futura interoperabilidade.

5. Conclusões

A partir dos resultados descritos, é possível concluir que a análise das médias e desvios padrões presentes no Experimento 1 refletem o primeiro indicativo de que é possível misturar assinaturas biométricas de teclados físicos e virtuais, mas com um processo de equalização dos intervalos DD por conta das médias distantes.

Prosseguindo com a apuração das informações obtidas, essa conclusão é ratificada pela análise dos histogramas e curvas gaussianas alcançadas no Experimento 2. Nota-se que os eventos DD e H, de fato, estão dentro dos padrões já conhecidos na literatura científica no que tange a distribuição log-normal proposta em [Montalvão Filho and Freire 2006] e [Montalvão et al. 2015]. Dessa forma, indica-se a adaptação dos dois tipos de teclados para uma subsequente concretização da interoperabilidade.

Por fim, é pertinente salientar a expectativa de altas acurácias da classificação do KNN encontradas no Experimento 3. Após a execução das repetições propostas, essa expectativa foi confirmada indicando facilidade em reconhecer assinaturas de cada dispositivo diferente. Além disso, é factual que os dados referentes aos intervalos DD + H e somente DD são muito parecidos. Este indicativo é reflexo do fato das informações discriminativas estarem principalmente nos intervalos DD. Conclui-se ainda que a menor acurácia foi para o intervalo H, o que demonstra semelhanças nos comportamentos deste evento entre as assinaturas obtidas por teclados de tipos distintos.

6. Perspectivas de futuros trabalhos

Visando o aprimoramento e continuidade desta pesquisa, e considerando os resultados obtidos até o presente momento, é proposto como trabalhos futuros: (a) a equalização dos intervalos DD, a fim de torná-los mais próximos em ambos os teclados e poder gerar assinaturas biométricas seguras, interoperáveis e individuais; (b) identificar as sessões da Base T (touchscreen), que não são indicadas de forma direta na base, assim como o processo de estabilização e esquecimento das assinaturas; (c) desenvolvimento de uma base de dados composta por assinaturas biométricas com o mesmo conjunto de autores, com o mesmo conjunto de eventos, tanto para teclados físicos quanto para touchscreens, a fim de tornar os experimentos mais seguros e de melhor qualidade.

Por fim, espera-se obter assinaturas keystroke únicas e interoperáveis entre teclados físicos e touchscreen, a fim de atenuar o problema de esquecimento nos dispositivos menos usados e aumentar o nível de segurança em acessos a sistemas com uma camada biométrica de baixo custo e confiável.

Referências

Antal, M., Szabó, L. Z., and László, I. (2015). Keystroke dynamics on android platform. *Procedia Technology*, 19:820–826.

Folha de S.Paulo (2023). Celular e tv são os equipamentos mais usados para acesso à internet no brasil. Acesso em: 7 jun. 2025.

Habeeb, A. (2019). Comparison between physiological and behavioral characteristics of biometric system. *Journal of Southwest Jiaotong University*, 54(6).

Killourhy, K. S. and Maxion, R. A. (2009). Comparing anomaly-detection algorithms for keystroke dynamics. In *2009 IEEE/IFIP international conference on dependable systems & networks*, pages 125–134. IEEE.

Montalvão, J., Freire, E. O., Bezerra Jr, M. A., and Garcia, R. (2015). Contributions to empirical analysis of keystroke dynamics in passwords. *Pattern Recognition Letters*, 52:80–86.

Montalvão Filho, J. R. and Freire, E. O. (2006). On the equalization of keystroke timing histograms. *Pattern Recognition Letters*, 27(13):1440–1446.

Shadman, R., Wahab, A. A., Manno, M., Lukaszewski, M., Hou, D., and Hussain, F. (2023). Keystroke dynamics: Concepts, techniques, and applications. *ACM Computing Surveys*.

Stragapede, G., Vera-Rodriguez, R., Tolosana, R., and Morales, A. (2023). Behavepassdb: public database for mobile behavioral biometrics and benchmark evaluation. *Pattern Recognition*, 134:109089.

TI Inside (2024). Uso da autenticação biométrica deve crescer cerca de 400% até 2027. Acesso em: 7 jun. 2025.

Xiaofeng, L., Shengfei, Z., and Shengwei, Y. (2019). Continuous authentication by free-text keystroke based on cnn plus rnn. *Procedia computer science*, 147:314–318.