/Rootəd CON

¿Y si conozco lo que tecleas? Un estudio de viabilidad

José Reverte Cazorla, José María de Fuentes, **Lorena González-Manzano**

lgmanzan@inf.uc3m.es
@LorenaGonzManz

uc3m


Stylish
HOME DESIGNS
Stylish Home Designs
Get inspired to live life in style.
- Stylish HOME DESIGNS

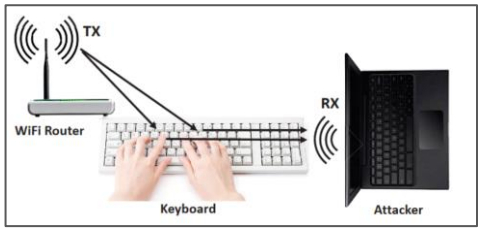
Objetivo

Ataques de canal lateral:

El atacante recopila datos extraídos indirectamente

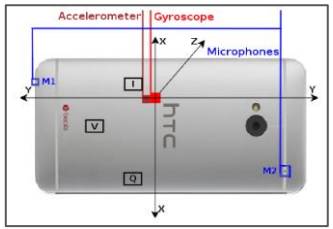
sin contacto directo con la víctima o su dispositivo

Basado en WiFi



Li et al. [1]

Basado en sensores



Narain et al. [2]

Basado en audio

Zhuang et al. [3]

Propuesta

Ataque de canal lateral en un teclado

- Teclado físico de un ordenador
- Cámara del portátil
- 50 teclas:
  - 10 dígitos, 27 letras (alfabeto español) y 13 símbolos
  - Sin limitaciones de entrada

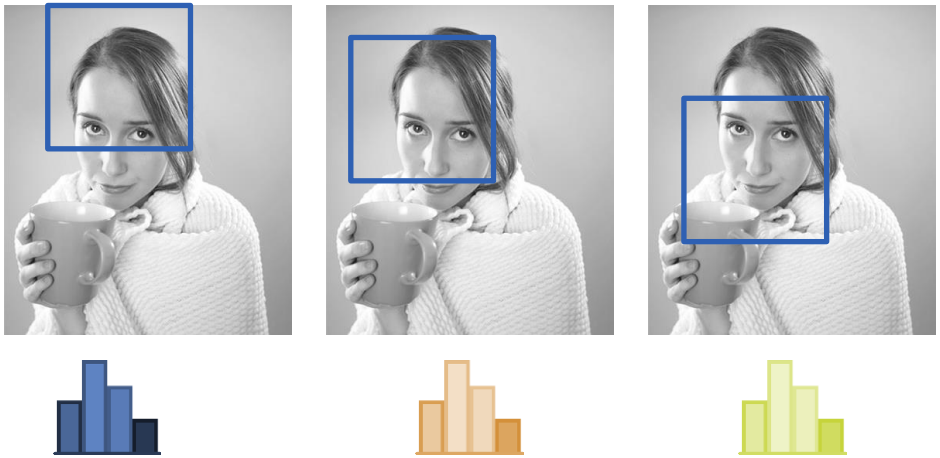
Objetivo principal:

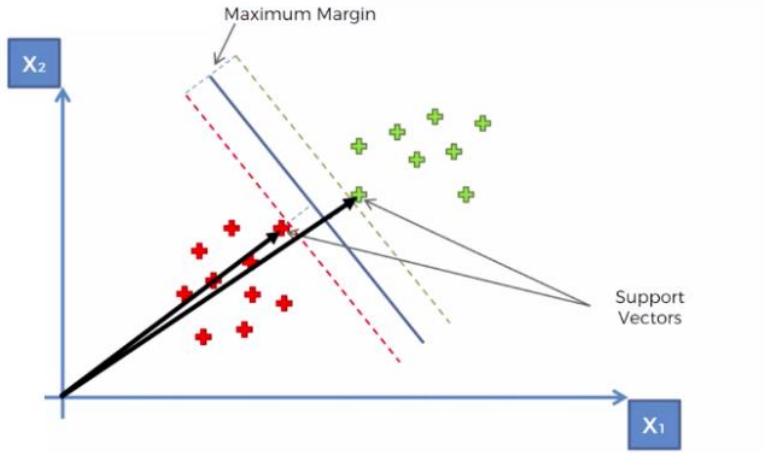
Evaluar la viabilidad de adivinar las pulsaciones de teclas mediante el análisis de una transmisión de video de la cara del usuario

Fundamentos

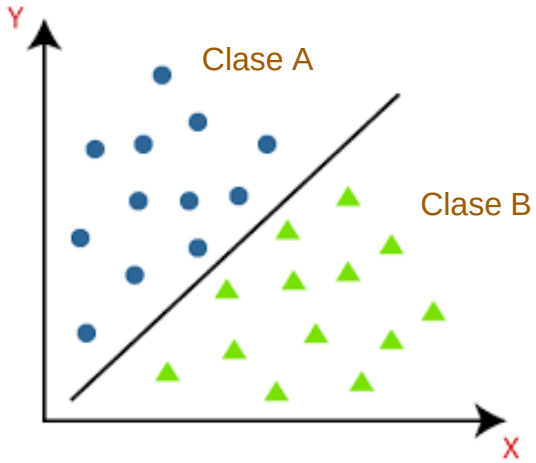
Técnicas de reconocimiento facil

Técnica de histograma de gradientes orientados + SVM lineal





Fundamentos



Clasificadores basados en Inteligencia artificial

Logistic Regression

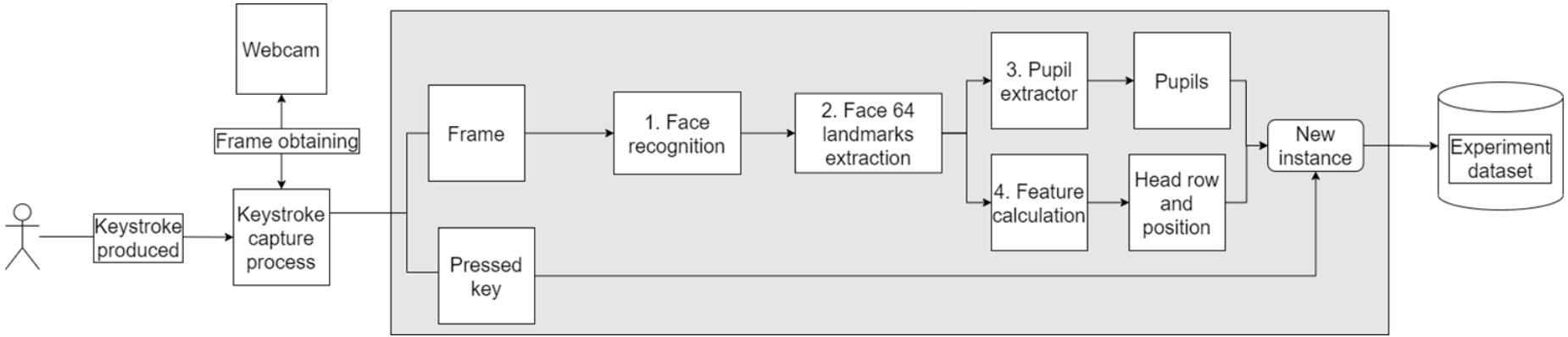
K-Nearest Neighbours

Support Vector Machine

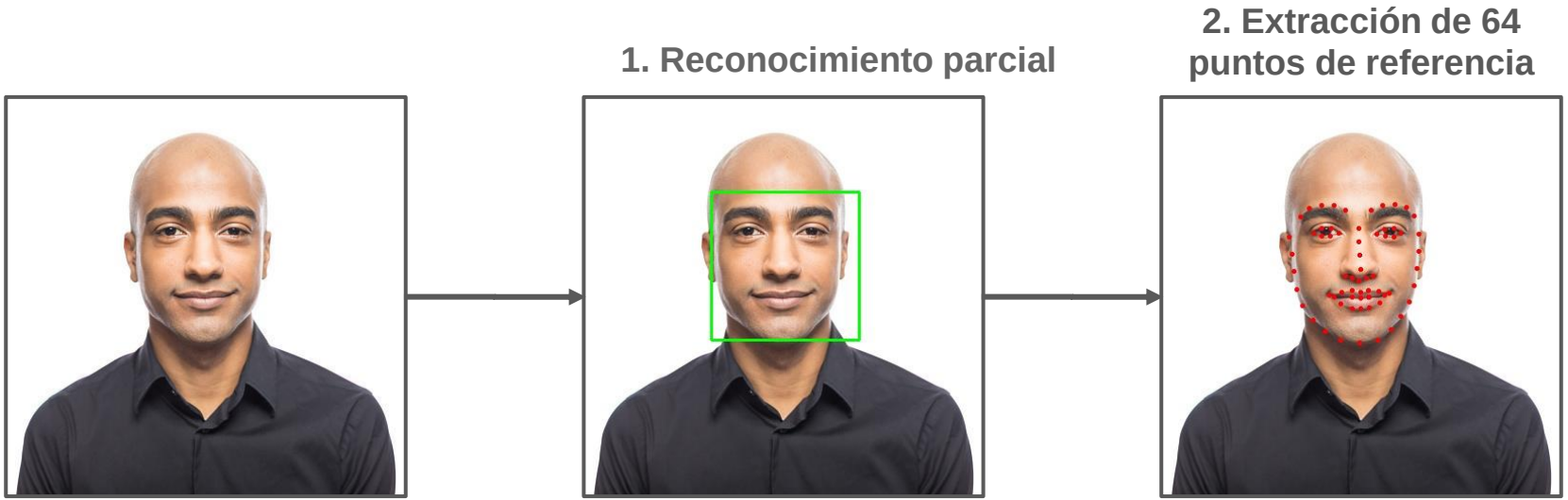
J48 (C4.5 implementation)

Logistic Model Tree

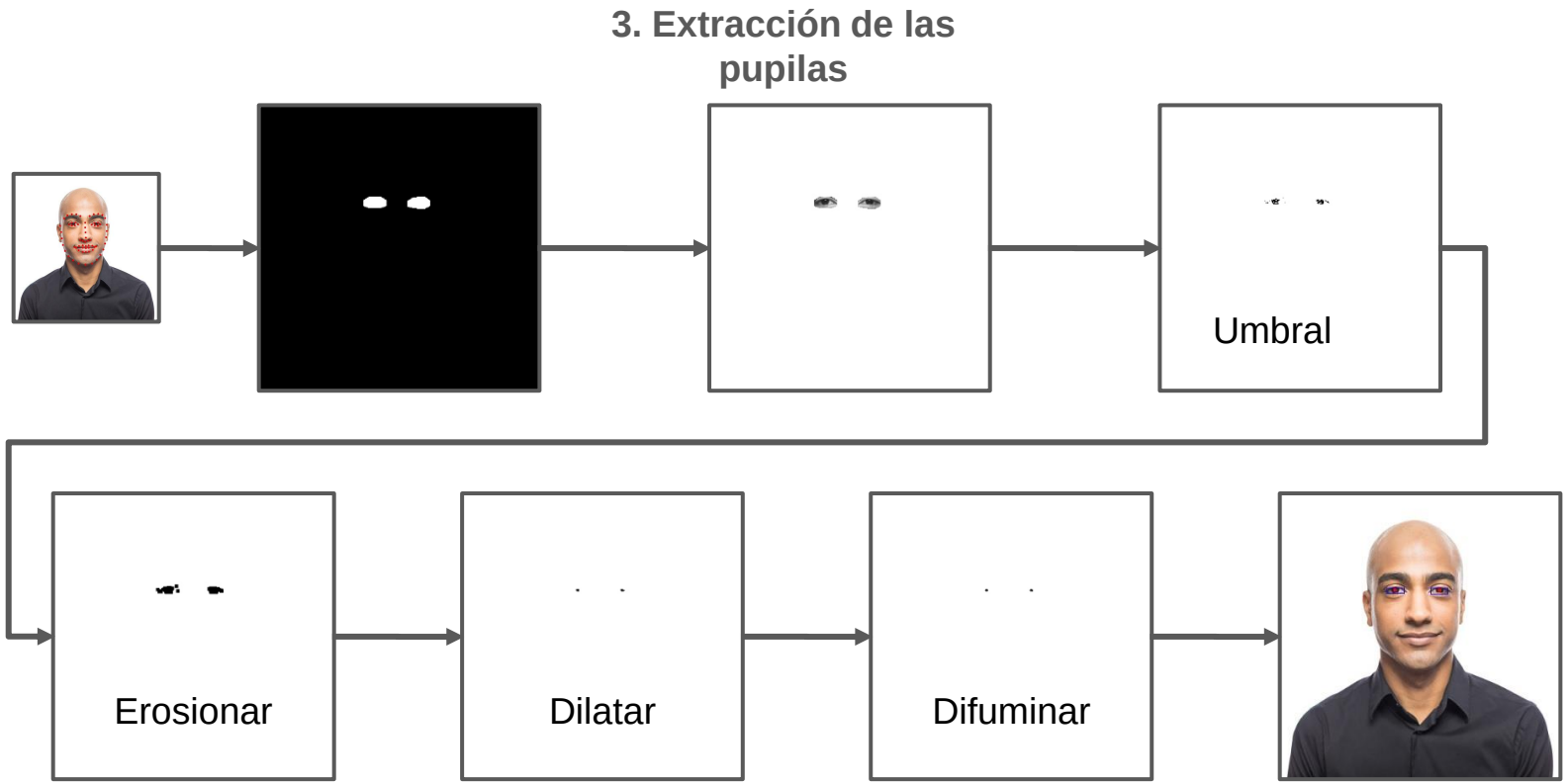
Descripción de la propuesta



Descripción de la propuesta

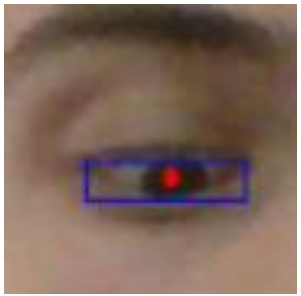


Descripción de la propuesta

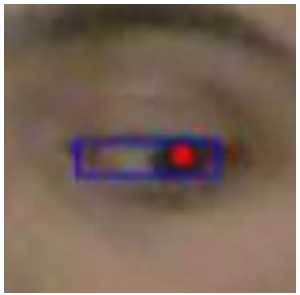


Descripción de la propuesta

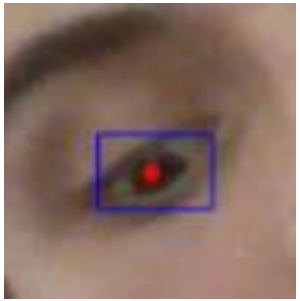
Mirando a la tecla ‘q’ (frame is x=640 y=480)



Mirar a x=459 y=245
(lado izq. del teclado)



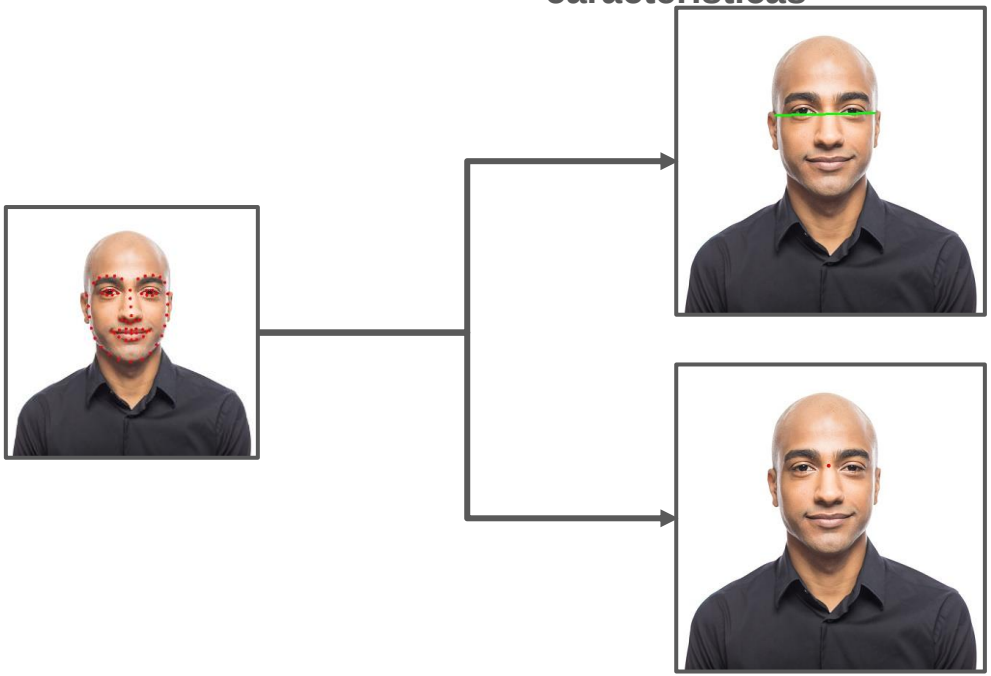
Mirar a x=97 y=194
(lado der. del teclado)



Cabeza inclinada 40.5
grados a la derecha

Descripción de la propuesta

4. Cálculo de características



Línea de la cabeza

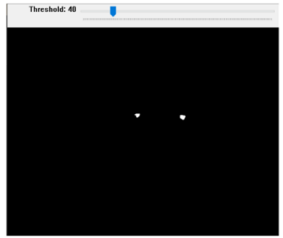
Posición de la cabeza

Proceso experimental

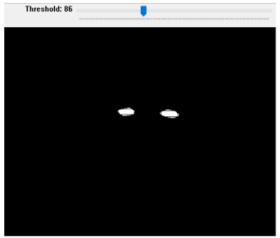
30 participantes

1. El usuario se adapta la silla al ordenador (portátil)
2. Comienza la extracción
3. Se ajusta el umbral.
4. El usuario escribe y finaliza con ‘ESC’

- 116 pruebas
- Textos entre 222 y 634 caracteres
- 58,384 pulsaciones recogidas, 49,635 tras el preprocesado



Óptima



Demasiado

Escaso

Proceso experimental. Configuración

Género		Edad		Gafas		Mirada		Luz		
M	F	Joven (17-28 años)	Mayor	Sí	No	Forzada	Natural	Natural	Oscura	Artificial
57	59	103	13	22	94	59	56	53	31	32

https://github.com/peperc/pupil-catcher

Proceso experimental. Parámetros y métricas

Algoritmo	Parámetros	Valores
LR	Ridge	1E-12,5, **10**
KNN	Neighbours	1, 32, **65**
J48	Confidence factor	**0.01**, 0.05, 0.1
J48	Minimum instances per leave	**6**, 9, 12
LMT	Minimum instances per leave	**1**, 15, 31
LMT	Trimming weight	**0**, 0.5, 1
SVM	Cost	**1**, 2.5, 5

Proceso experimental. Resultados y análisis

Precisión

		Género		Edad		Gafas		Luz		
	Todas	M	F	Joven	Mayor	Sí	No	Natural	Oscura	Artificial
KNN	13.69	14.47	13.31	13.28	13.63	13.03	13.63	14.57	15.01	12.91
J48	13.71	14.98	13.38	12.99	13.94	13.48	14.51	14.88	14.78	13.0
LMT	13.3	15.09	13.03	12.37	13.71	13.27	14.05	14.42	14.12	12.13
LR	11.05	10.56	11.59	12.7	10.94	12.88	10.59	10.52	12.24	11.01
SVM	13.38	12.62	14.22	11.45	13.56	12.3	13.58	12.63	12.78	10.69

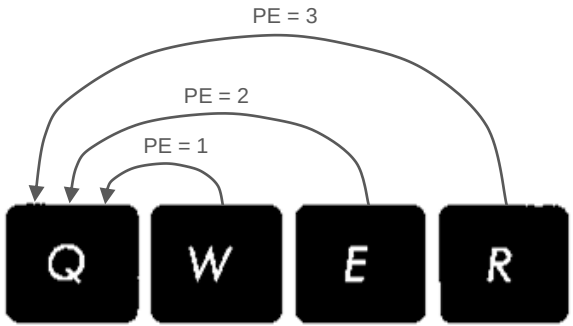
Proceso experimental. Resultados y análisis

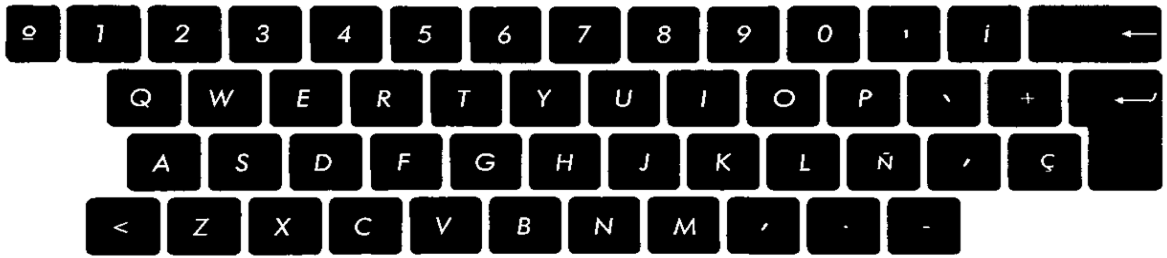
Precisión

		Género		Edad		Gafas		Luz		
	Todas	M	F	Joven	Mayor	Sí	No	Natural	Oscura	Artificial
KNN	13.69	14.47	13.31	13.28	13.63	13.03	13.63	14.57	15.01	12.91
J48	13.71	14.98	13.38	12.99	13.94	13.48	14.51	14.88	14.78	13.0
LMT	13.3	15.09	13.03	12.37	13.71	13.27	14.05	14.42	14.12	12.13
LR	11.05	10.56	11.59	12.7	10.94	12.88	10.59	10.52	12.24	11.01
SVM	13.38	12.62	14.22	11.45	13.56	12.3	13.58	12.63	12.78	10.69

Proceso experimental. Resultados y análisis

Posibles tipos de error:

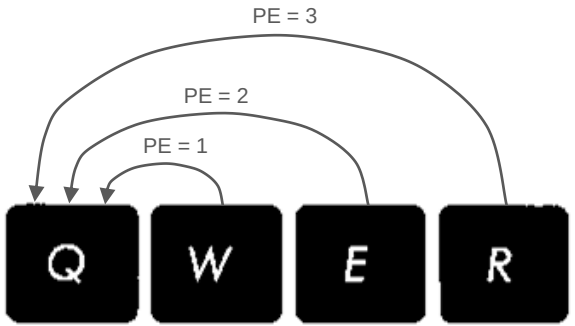




Proceso experimental. Resultados y análisis

Precisión

		Género		Edad		Gafas		Luz		
J48	Todas	M	F	Joven	Mayor	Sí	No	Natural	Oscura	Artificial
PE=0	13.71	14.98	13.38	12.99	13.94	13.48	14.51	14.88	14.78	13.0
PE≤1	31.76	33.69	31.91	18.38	32.13	17.27	32.96	33.15	34.88	31.63
PE≤2	52.50	53.02	53.22	35.43	52.66	36.49	53.33	53.05	55.0	52.27
PE≤3	61.25	61.99	61.62	52.75	61.43	54.43	62.53	61.81	62.93	60.8



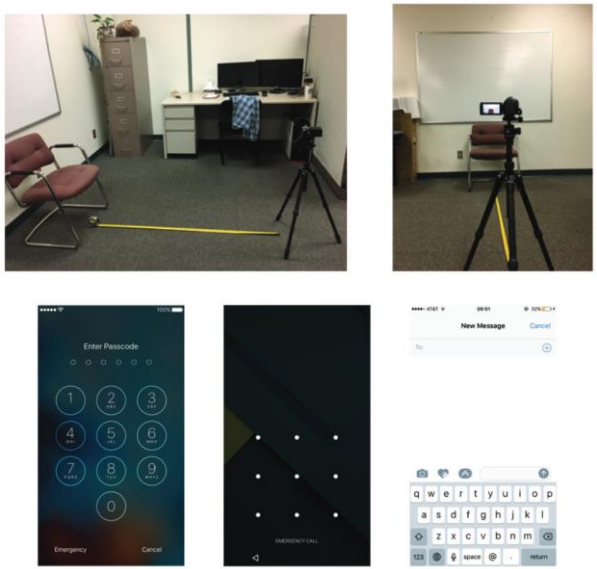
Proceso experimental. Resultados y análisis

Precisión

			Género		Edad		Gafas		Luz		
J48		Todas	M	F	Joven	Mayor	Sí	No	Natural	Oscura	Artificial
Mirada forzada	PE=0	15.79	18.05	14.87	12.1	16.71	12.36	17.07	18.56	15.46	14.86
	PE≤1	34.84	36.99	33.86	22.14	35.69	20.45	37.26	37.57	37.26	35.99
	PE≤2	54.19	55.61	43.54	33.1	55.11	39.98	55.39	55.77	58.54	55.72
	PE≤3	63.98	64.71	57.68	42.35	64.89	62.93	65.27	65.26	65.9	65.16
Mirada natural	PE=0	13.21	13.8	13.26	14.67	13.39	14.91	13.25	13.67	15.1	13.13
	PE≤1	31.65	33.11	31.25	21.44	31.87	18.97	31.66	32.56	35.16	20.27
	PE≤2	52.82	54.06	52.25	40.37	52.7	28.38	52.67	52.95	54.62	30.88
	PE≤3	60.02	60.77	60.07	60.69	60.26	44.1	60.44	59.95	63.05	47.11

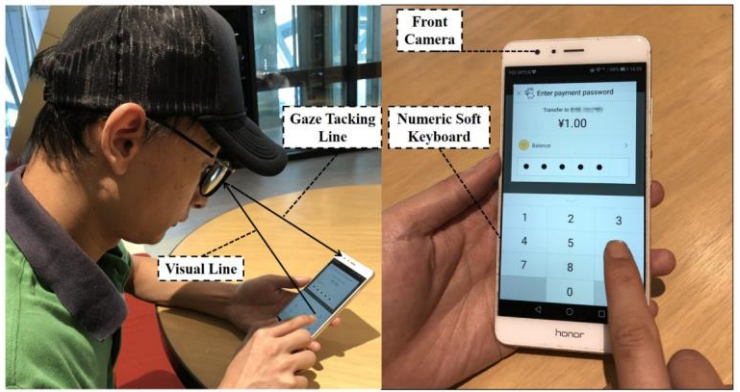
Trajos relacionados - Novedad

EyeTell[4]



(a) PIN (b) Pattern lock (c) Alphabetical

GazeRevealer[5]



Conclusiones

- Estudio de la viabilidad – obtención pulsaciones teclado a través de la cámara web
- Uso de un teclado “típico”
- Caracterización por múltiples factores
- Con 1 error > 30% de acierto

Limitaciones

Mirada en la pantalla
Gafas
Dirección/ Distancia de la luz

Trabajo futuro

Procesamiento de lenguaje natural
Tipo/ Diseño de teclado
Mejora del preprocesado

References

1. M. Li, Y. Meng, J. Liu, H. Zhu, X. Liang, Y. Liu, and N. Ruan, “When csi meets public wifi: Inferring your mobile phone password via wifi signals,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS ’16. New York, NY, USA: Association for Computing Machinery, 2016, p. 1068–1079. [Online]. Available: https://doi.org/10.1145/2976749.2978397
2. S. Narain, A. Sanatinia, and G. Noubir, “Single-stroke language-agnostic keylogging using stereo-microphones and domain specific machine learning,” in Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless; Mobile Networks, ser. WiSec ’14. New York, NY, USA: Association for Computing Machinery, 2014, p. 201–212. [Online]. Available: https://doi.org/10.1145/2627393.2627417
3. L. Zhuang, F. Zhou, and J. D. Tygar, “Keyboard acoustic emanations revisited,” ACM Transactions on Information and System Security (TISSEC), vol. 13, no. 1, pp. 1–26, 2009.
4. Y. Chen, T. Li, R. Zhang, Y. Zhang, and T. Hedgpeth, “Eyetell: Video-assisted touchscreen keystroke inference from eye movements,” in 2018 IEEE Symposium on Security and Privacy (SP), 2018, pp. 144–160.
5. Y. Wang, W. Cai, T. Gu, and W. Shao, “Your eyes reveal your secrets: An eye movement based password inference on smartphone,” IEEE Transactions on Mobile Computing, vol. 19, no. 11, pp. 2714–2730, 2020.

/Rootəd CON

¿Y si conozco lo que tecleas? Un estudio de viabilidad

José Reverte Cazorla, José María de Fuentes, **Lorena González-Manzano**

lgmanzan@inf.uc3m.es
@LorenaGonzManz

uc3m