Ciencias Matemáticas, Vol. 35, No. 1, 2021, Pag. 27-35
Recibido 11-2020, Aceptado 04-2021

Midiendo la legitimidad del usuario autenticado en sistemas de Autenticación Gráfica "Cued Recall". Measuring the legitimacy of the authenticated user in systems of Graphic Authentication "Cued Recall".

Pedro Enrique Navarro Sosa[1]*, Carlos Miguel Legón Pérez[1], Raisa Socorro Llanes[2]

Resumen La Autenticación Gráfica es un tema muy actual sobre la que se publican numerosas investigaciones. Recientemente se propuso un modelo probabilístico para medir la autenticidad del usuario en sistemas de autenticación gráfica "Cued Recall" que emplean discretización centrada o robusta. Ese modelo aporta una métrica para medir el grado de autenticidad de los usuarios (legítimos o no) que logran autenticarse en este tipo de sistema, sin embargo, una limitación del modelo anterior es que se desconoce la distribución del estadígrafo propuesto. En este trabajo se obtiene la distribución teórica de ese estadígrafo, mediante la aplicación de 3 test de bondad de ajuste a más de 50 distribuciones conocidas, A partir de esta distribución se modifica, mejora en el modelo anterior el criterio de selección de los umbrales empleados para evaluar el grado de autenticidad del usuario, lo cual contribuye a mejorar su generalización y aplicación práctica. Se confirma experimentalmente la efectividad de la modificación propuesta.

Abstract Graphical Authentication is a very current topic on which numerous investigations are published. A probabilistic model was recently proposed to measure user authenticity in "Cued Recall" graphical authentication systems that employ focused or robust discretization. This model provides a metric to measure the degree of authenticity of the users (legitimate or not) who manage to authenticate in this type of system, however, a limitation of the previous model is that the distribution of the proposed statistician is unknown. In this work, the theoretical distribution of this statistician is obtained by applying 3 goodness-of-fit tests to more than 50 known distributions.From this distribution, the selection criteria for the thresholds used are modified and improved in the previous model. to evaluate the degree of authenticity of the user, which contributes to improve its generalization and practical application. The effectiveness of the proposed modification is confirmed experimentally.

Palabras Clave / Keywords
Autenticación Gráfica / Graphical Autentication - Modelo Probabilístico / Probabilistic Model - Cued Recall

[1] *Instituto de Criptografía, Universidad de La Habana, La Habana, Cuba, pedropepe3437@gmail.com, mgp@aguacate.edu.cu*
[2] *Facultad de Ingeniería Informática, Universidad Tecnológica de La Habana, La Habana, Cuba, jgp@mamonzillo.edu.cu*
***Autor para Correspondencia**

Introducción

Los Sistemas de Autenticación Gráfica son una alternativa viable a la autenticación por contraseñas alfanuméricas y constituyen actualmente un área activa de investigación. En los Sistemas de Autenticación Gráfica del tipo "Cued Recall", la contraseña del usuario consiste en k puntos S_i que este selecciona, en la fase de registro, de una o varias imágenes. Para autenticarse, el usuario debe escoger en el orden correcto, k puntos Q_i que deben coincidir (aproximadamente) con los S_i.

Existen ataques de diccionario contra estos sistemas de Autenticación Gráfica [1], que logran autenticarse con ciertas probabilidades de éxito, que dependen de la calidad del diccionario construido. A pesar de que no existen bases de datos de contraseñas gráficas, estos diccionarios se construyen a partir de la información obtenida por tres vías, primero la existencia de puntos más probables en la imagen ("hotspots") [2] , segundo, la información que guardan en claro los métodos de discretización [3] y tercero, la existencia de patrones en las contraseñas escogidas por los usuarios (contraseñas débiles) [4] [5]. Recientemente en [6] se propuso un nuevo modelo probabilístico para medir el grado de autenticidad de los usuarios que son autenticados en los sistemas de Autenticación Gráfica "Cued Recall", que emplean discretización centrada o la óptima. Lo denotaremos por modelo L. Este modelo construye un estadígrafo máximo verosímil basado en las distancias $d_i = d(S_i, Q_i)$ entre los puntos S_i de registro y los puntos Q_i de autenticación. El modelo L es aplicable solo en estos tipos de discretización, pues una vez que el usuario es autenticado, el centro de la región de tolerancia de cada punto Q_i será igual al punto S_i y a partir de ellos se puede calcular la distancia d_i. No conocemos antecedentes de modelos de ese tipo en Autenticación Gráfica. Su ventaja principal

es que aporta una nueva medida del nivel de autenticidad del usuario autenticado, lo cual podría ser empleado para detectar ataques de diccionario exitosos contra este tipo de sistema, sin embargo, una limitación del modelo L es que se desconoce la distribución del estadígrafo propuesto. En este trabajo se determinó la distribución teórica del estadígrafo propuesto en el modelo L, y se demuestra experimentalmente que su aplicación permite escoger con mayor rigor teórico los umbrales para medir el nivel de autenticidad del usuario autenticado, reduciendo así en la practica la probabilidad de error en la clasificación de los usuarios.

1. Preliminares

1.1 Autenticación Gráfica "Cued Recall".

Estos sistemas Autenticación Gráfica requieren que el usuario memorice un conjunto de puntos en áreas predeterminadas de una imagen o conjuntos de ellas. En la idea original [7], el usuario debía marcar con un mouse o un lapicero en determinados puntos de una imagen, si lo hacía de forma correcta este sería aceptado por el sistema de lo contrario sería rechazado. Los mismos cuentan con 2 fases principales, fase de registro y fase de autenticación. [8] [9]

En la fase de registro, el usuario escoge k puntos, pero el sistema por seguridad, no guarda en texto claro los k puntos, ni sus regiones de tolerancia, lo que guarda es el $Hash(RT_1,\ldots,RT_k)$ de la concatenación ordenada de las k regiones de tolerancia RT_i determinadas por la contraseña.

En la fase de autenticación. El usuario es autenticado si y solo si el hash de la fase de registro coincide con el hash de la fase de autenticación. Esto equivale a que todos los puntos Q_i escogidos en la fase de registro pertenecen a la región de tolerancia de los puntos escogidos en la fase de registro.

Se espera que el usuario legítimo recuerde aproximadamente el orden y la posición de los k pixeles S_i que el escogió en la fase de registro, pero es muy poco probable que logre recordar de forma exacta la posición de cada pixel, por esta razón la imagen se discretiza y se define una región de tolerancia RT alrededor de cada punto. Los principales métodos de discretización empleados en estos sistemas para definir la región de tolerancia RT son la Discretización Robusta [10], la Centrada [11] y la Óptima [12]. Una descripción detallada de ellas y una discusión de sus limitaciones puede verse en [3].

Como se observa, el criterio esencial para autenticar un usuario es que todos los puntos Qi de la fase de autenticación estén cerca de su correspondiente punto Pi escogido en la fase de registro.

1.2 El Modelo L

En [13] se señala como una limitación de los métodos de Autenticación Gráfica "Cued Recall", que la distancia $d_i = d_i(S_i,Q_i)$ se tiene en cuenta solo para autenticar o no al usuario, pero no se tienen en cuenta sus diferencias dentro de la región de tolerancia RT entre los usuarios ya autenticados. Partiendo de las características del proceso de autenticación en los sistemas de Autenticación Gráfica "Cued Recall", se imponen 4 condiciones (axiomas), que debe cumplir una distribución de probabilidades $P(d_i)$ dentro de la región de tolerancia RT para medir en cada distancia di, el grado de autenticidad de un usuario.

- Las condiciones 1 y 2 son las comunes a cualquier modelo probabilístico, para garantizar que $P(d_i)$ sea una distribución de probabilidades sobre todos los puntos de la imagen.
- Las condiciones 3 y 4 son específicas de este problema y significan que un pequeño grupo de las menores distancias $d_i = d(S_i,Q_i)$ entre los puntos S_i de registro y los puntos Q_i de autenticación, deben tener asignada muy alta probabilidad. Estas condiciones sugieren una forma para la distribución buscada y a partir de esa sugerencia se propone una función que cumple estas condiciones para cada $d_i = d(S_i,Q_i)$.

A partir de la función propuesta para cada punto y asumiendo independencia entre los puntos de la contraseña, se propone un estadígrafo de verosimilitud:

$$L_2(Q) = \left(\frac{max_{S_0\in I_{mxn}} L_1(S_0) - L_1(Q)}{max_{S_0\in I^k_{mxn}} L_1(S_0) - min_{S_0\in I^k_{mxn}} L_1(S_0)}\right) * C_L \quad (1)$$

Dónde $max_{S_0\in I_{mxn}}$ es la distancia de S al pixel de la imagen más lejano de la imagen, $min_{S_0\in I^k_{mxn}} = 0$, I_{mxn} es la imagen de tamaño nxm pixeles y $L_1(Q)$ es:

$$L_1(Q) = \sum_{i=1}^{k} logP(Q_i) \quad (2)$$

Dado un punto Q_i, se calcula su distancia a S_i y a partir de ella, se calcula su probabilidad $P(Q) = P(Q_i = P_i)) = P(d(Q_i,S_i))$. Y estas últimas probabilidades se definen en [13] de forma que cumplan las condiciones 1-4 anteriormente mencionadas. Por propiedades del logaritmo $L_1(Q)$ toma valores negativos. Por razones de implementación, para trabajar con valores enteros positivos, se selecciona una constante $C_L \in N$.

La ventaja de este estadígrafo es que logra distinguir el nivel de autenticidad de los usuarios ya autenticados y puede aplicarse para resolver un problema de hipótesis del tipo:

H_0**:** El usuario autenticado es legítimo.

H_1**:** El usuario autenticado no es legítimo.

Su principal limitación es que no se conoce su distribución teórica y por tanto la elección de la región crítica debe hacerse mediante simulación.

Los grupos de contraseñas G_1 y G_2, empleados en [13] también se emplearán en este trabajo y están definidos de la siguiente forma:

Grupo G_1**:** Este grupo simula a un usuario legítimo, que recuerda muy bien su contraseña. La contraseña $Q = (q_1,...,q_5)$ propuesta por el usuario que intenta autenticarse está formada por 5 puntos dentro de la región de tolerancia que además estarán todos muy cercanos al punto correspondiente de la contraseña S, en particular $d(Q_i,S_i) \leq 5$.

Grupo G_2: Simula a un usuario legítimo, que no recuerda muy bien su contraseña. Los 5 puntos $Q = (q_1, ..., q_5)$ estarán dentro de la región de tolerancia pero lejos del punto correspondiente de la contraseña S, a una distancia $5 < d(Q_i, S_i) \leq 10$.

1.3 Software EasyFit

EasyFit [14] es un programa que permite encontrar las distribuciones estadísticas que mejor se ajustan a la serie de datos introducida. El programa representa las leyes de densidad y de distribución gráficamente, por lo que ya se puede obtener una estimación de su ajuste por medios visuales. Analíticamente, proporciona los resultados obtenidos por los test de ajustes de Kolmogorov-Smirnov, Anderson-Darling y Chi cuadrado.

A continuación en el cuadro 1 se nombran las 54 distribuciones a las cuales el software EasyFit mide el ajuste de la muestra estudiada:

Hyperbolic Secant	Beta	Binomial
Discrete Uniform	Burr	Cauchy
Chi-Squared	Dagum	Erlang
Error Function	Error	Gamma
Exponential	Frechet	Bernoulli
Gen. Extreme Value	F	Geometric
Gen. Gamma	Gumbel Max	Gumbel Min
Gen. Logistic	Nakagami	Levy
Gen. Pareto	Johnson SB	Johnson SU
Negative Binomial	Fatigue Life	Laplace
Log-Pearson 3 (LP3)	Logarithmic	Logistic
Phased Bi-Exponential	Lognormal	Pert
Phased Bi-Weibull	Log-Gamma	Log-Logistic
Inverse Gaussian	Kumaraswamy	Normal
Pareto 2 (Lomax)	Pareto	Poisson
Hypergeometric	Rayleigh	Rice
Student's t	Triangular	Uniform
Reciprocal	Wakeby	Weibull

Cuadro 1. Las 54 distribuciones contenidas en "EasyFit"

2. Resultados y Discusión

2.1 Estimación de la distribución del estadígrafo propuesto en el modelo L

En este epígrafe se aplicaron varios test de bondad de ajuste a una muestra del estadígrafo propuesto en el modelo L, comparándola con distribuciones teóricas conocidas, encontrando una distribución teórica a la cual esa muestra posee ajusta. Este resultado constituye un aporte notable al modelo anterior, pues permite calcular teóricamente los p-valores o umbrales empleados para evaluar el grado de autenticidad del usuario, lo cual contribuye a mejorar su generalización y aplicación práctica.

2.1.1 Diseño del experimento 1

Construcción de la muestra. Se implementó una versión básica de un sistema de Autenticación Gráfica "Cued Recall". Con este sistema se generó una muestra de $M = 1000$ parejas de contraseñas gráficas del tipo (fase registro, fase autenticación), correspondientes a un usuario legítimo del G_1. A cada una de ellas se le aplicó el modelo L y se obtuvo una muestra de L valores de su estadígrafo.

Evaluación de la muestra. A esta muestra de M=1000 valores del estadígrafo, se le aplico el software "EasyFit"para obtener los gráficos y los P-valores de las distribuciones evaluadas en este software para cada uno de los 3 test de bondad de ajuste Kolmogorv Smirnov(KS), Anderson Darling(AD), y Chi-Cuadrado(CH-C).

- Primera elección. Se seleccionaron las 20 distribuciones con valores más altos de sus estadígrafos KS. Se emplearon 5 niveles de significación diferentes $\alpha \in (0{,}2, 0{,}1, 0{,}05, 0{,}02, 0{,}01)$ para comparar con los P-valores obtenidos y medir el ajuste a cada distribución.
- En una segunda selección, se escogieron las 6 mejores de esas 20 y esas 6 distribuciones se compararon según el número de rechazos de la hipótesis de ajuste (entre todos los niveles de significación $\alpha \in (0{,}2, 0{,}1, 0{,}05, 0{,}02, 0{,}01)$ y los 3 test KS, AD, CH-C) y según la magnitud decreciente de sus P-valores para cada test. A partir de los resultados obtenidos se escogió, entre esas 6, cual es la distribución teórica a la cual ajusta mejor la muestra de 1000 valores del estadígrafo del modelo L.

2.1.2 Las 20 distribuciones teóricas con mejor ajuste

A continuación, en la figura 1 se muestran las 20 distribuciones teóricas a las que mejor ajustó la muestra de $M = 1000$ observaciones obtenidas a partir del estadígrafo del modelo L, según el test de Kolmogorv Smirnov, ordenadas por el valor de su estadígrafo. Se muestra, además, para cada una de ellas el valor del estadígrafo de los test de Anderson Darling y Chi-Cuadrado, así como el rango que les corresponde según ese estadígrafo.

Discusión de los resultados. Las 20 distribuciones anteriores, fueron escogidas por el test Kolmogorv Simrnov, pero al evaluar su rango por los test Anderson Darling y Chi-cuadrado se observa que solo 3 de ellas están fuera del rango 1-20 según esos dos test. Por lo tanto, los 3 test coinciden en que estas son las distribuciones que más ajustan. A partir de este análisis se limitará el estudio a las distribuciones de las 6 primeras filas.

Distribución	Kolmogorov Smirnov		Anderson Darling		Chi-cuadrado	
	Estadística	Rango	Estadística	Rango	Estadística	Rango
Gen. Extreme Value	0,01891	1	16,168	31	N/A	
Johnson SB	0,02129	2	0,32635	3	5,124	1
Kumaraswamy	0,02209	3	0,34584	4	6,0163	2
Beta	0,02445	4	2,7882	7	11,22	4
Weibull (3P)	0,025	5	0,7193	5	6,766	3
Weibull	0,02756	6	0,8091	6	11,296	5
Log-Pearson 3	0,02921	7	40,364	38	N/A	
Log-Logistic (3P)	0,04849	8	4,5044	9	33,622	8
Erlang (3P)	0,04987	9	5,2062	15	46,258	17
Inv. Gaussian (3P)	0,05098	10	4,1771	8	36,45	12
Gumbel Min	0,05221	11	4,707	12	34,809	11
Inv. Gaussian	0,05563	12	11,498	25	73,647	23
Gen. Gamma (4P)	0,05626	13	4,7349	13	34,32	9
Normal	0,05627	14	4,5216	10	32,458	6
Fatigue Life (3P)	0,05685	15	4,618	11	32,473	7
Lognormal (3P)	0,06156	16	5,7235	16	42,666	14
Error	0,0618	17	4,9047	14	34,436	10
Gen. Pareto	0,06205	18	249,67	46	N/A	
Pearson 5 (3P)	0,06319	19	7,0587	18	57,947	19
Gamma (3P)	0,0664	20	7,0086	17	55,895	18

Figura 1. Las 20 distribuciones teóricas a las cuales la muestra mostró mayor ajuste, entre las 54 evaluadas en EasyFit.

2.1.3 Comparación del Histograma del estadígrafo L en el G_1 con las 6 distribuciones a las que mejor se ajusta la muestra.

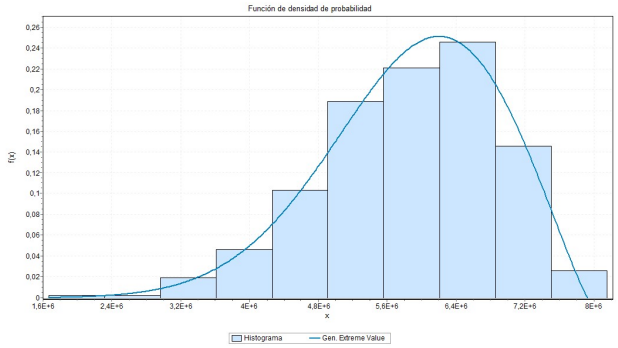

Figura 2. Ajuste de la muestra a la distribución Gen. Extreme Value.

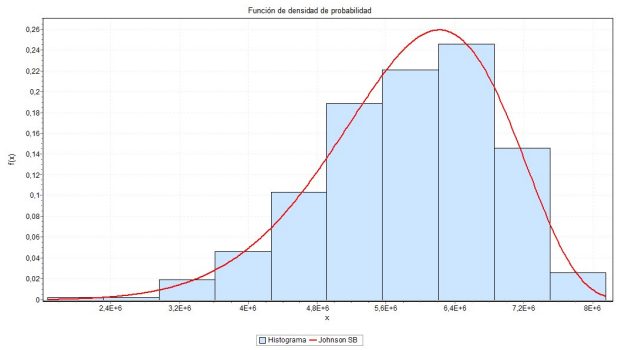

Figura 3. Ajuste de la muestra a la distribución Johnson SB.

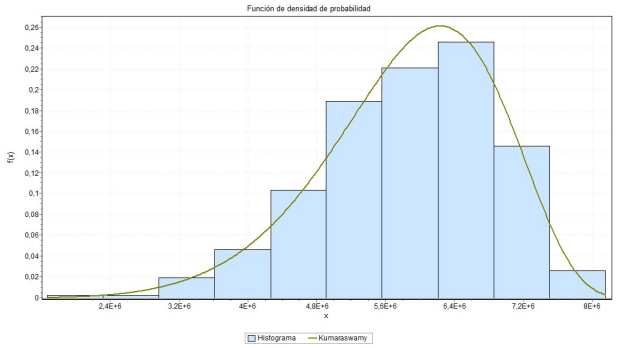

Figura 4. Ajuste de la muestra a la distribución Kumaraswamy.

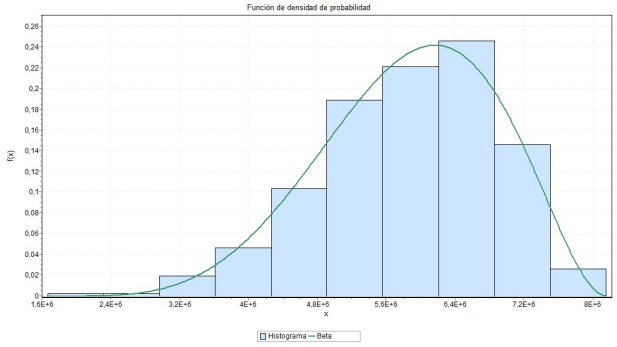

Figura 5. Ajuste de la muestra a la distribución Beta.

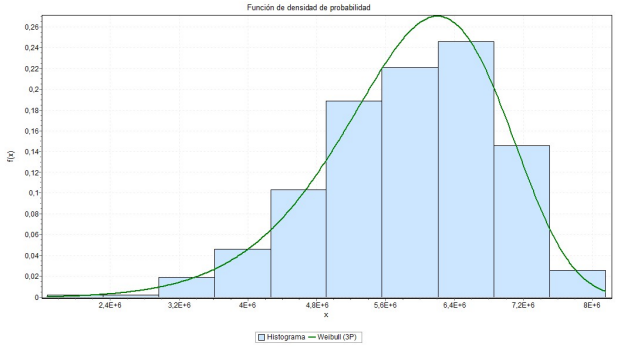

Figura 6. Ajuste de la muestra a la distribución Weibull (3P).

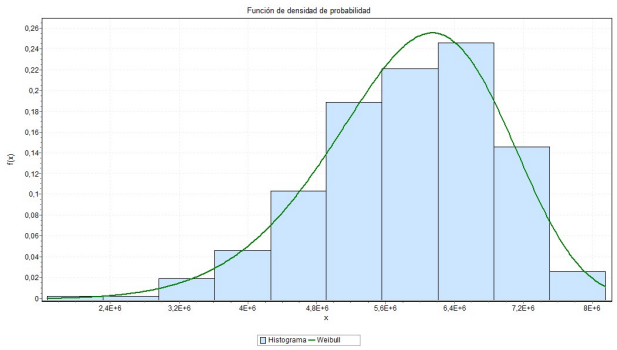

Figura 7. Ajuste de la muestra a la distribución Weibull.

Discusión de los resultados. El análisis visual de los 6 histogramas mostrados previamente sugiere que la muestra presenta un buen ajuste a cada una de estas 6 distribuciones. Para facilitar la comparación, en la siguiente figura 8 se muestra el histograma comparado con las 6 distribuciones simultáneamente.

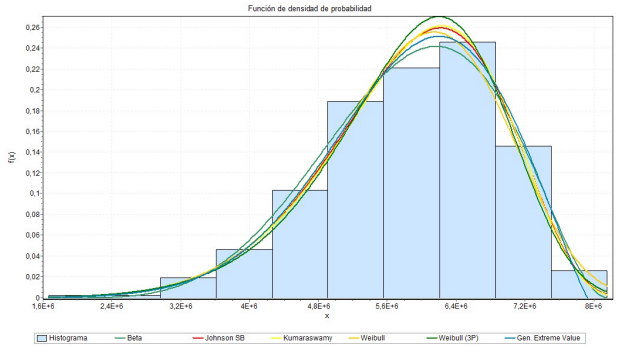

Figura 8. Las 6 distribuciones, entre las 20 de la Figura 1, a las cuales la muestra se ajusto mejor.

Aunque se observan algunas diferencias en el ajuste en la cola derecha y en la parte superior del histograma, estas son insuficientes para detectar visualmente diferencias en el nivel de ajuste, por lo tanto, se continuara la comparación usando los P-valores obtenidos para los test KS y CH-C.

2.1.4 Comparación del grado de Ajuste de la muestra a las 6 distribuciones que mejor ajustan

El ajuste de la muestra a cada distribución teórica se evalúa 15 veces, empleando los 5 niveles de significación $\alpha \in (0{,}2; 0{,}1; 0{,}05; 0{,}02; 0{,}01)$ para cada test (KS, AD, CH-C).

Distribución	KS	CH-C	No. Rechazos
Johnson SB	0,74667	0,82337	0/15
Kumaraswamy	0,70488	0,73829	0/15
Weibull 3P	0,551	0,66147	0/15
Weibull	0,42585	0,25596	0/15
Gen Extreme Value	0,85998	N/A	5/10
Beta	0,57985	0,26093	3/15

Cuadro 2. Los 12 P-valores asociados a la muestra, para 6 distribuciones y los 2 test de bondad de ajuste KS y CH-C.

Discusión de los resultados. Las 6 distribuciones del cuadro 2 se pueden dividir en 3 grupos. Inicialmente en 2 grupos atendiendo al número de rechazos del ajuste (columna 4). El peor grupo está formado por las distribuciones Gen. Extreme Value y Beta de las dos últimas filas, para las cuales se rechaza el ajuste en al menos un test, con 3 o más de los 5 valores de significación prefijados (Anexo 1). Para las restantes 4 distribuciones (filas 1-4) Johnson SB, Kumaraswamy, Weibull(3P) y Weibull no se rechaza el ajuste de la muestra a las distribuciones por ninguno de los 3 test, para ninguno de los 5 P-valores prefijados. Por esta razón, se descartan las 2 últimas y se reduce el análisis a estas 4 primeras distribuciones.

Esas 4 primeras distribuciones, se pueden separar en 2 grupos atendiendo a la magnitud de sus P-valores en los tests de bondad de ajuste KS y CH-C. El peor grupo está formado por las distribuciones Weibull(3P) y Weibull(filas 3-4) con P-valores por debajo de 0.7. El mejor grupo está formado por las dos primeras distribuciones Johnson SB y Kumaraswamy, con P-valores por encima de 0.7, pero entre ellas dos destaca el ajuste a JohnsonSB, con P-valores iguales a 0.74667 para el test KS y 0.82337 para el test Anderson Darling.

Conclusión del epígrafe. Los resultados alcanzados permiten concluir que, para los niveles de significación $\alpha \in (0{,}2, 0{,}1, 0{,}05, 0{,}02, 0{,}01)$, la muestra de valores del estadígrafo propuesto en el modelo L se ajusta a una distribución Johnson SB. La muestra de valores del estadígrafo del G_1 se ajusta a la distribución Johnson SB con estos parámetros:

- $\gamma = -2{,}0746$
- $\delta = 2{,}0934$
- $\lambda = 1{,}0875E+7$
- $\xi = -1{,}9534E+6$

Se denotará por L-JSB al estadígrafo del modelo L, después de aplicarle la transformación JSB.

2.2 Aplicación del estadígrafo L-JSB para medir la autenticidad del usuario

2.2.1 Distribución Johnson SB

Se dice que una muestra de datos no-normales de la variable X se ajusta a la distribución Johnson SB si realizando a los datos X la transformación Johnson SB los datos Z obtenidos después de la trasformación siguen una distribución Normal $N(0,1)$. La transformación depende de varios parámetros, que deben ser estimados a partir de la muestra.

Parámetros: $\gamma; \delta; \lambda; \xi$ donde $(\delta, \lambda) > 0$

Dominio: $\xi \leq x \leq \xi + \lambda$

Función de Densidad de Probabilidad:

$$f(x) = \frac{\delta}{\lambda\sqrt{2\pi z(1-z)}} exp(-\frac{1}{2}(\gamma + \delta ln(\frac{z}{1-z}))^2) \qquad (3)$$

Función de Distribución Acumulativa:

$$F(x) = \phi(\gamma + \delta ln(\frac{z}{1-z})) \qquad (4)$$

donde

$$z \equiv \frac{x-\xi}{\lambda} \qquad (5)$$

y ϕ es la Integral de Laplace.

2.2.2 Diseño del Experimento 2

Objetivo del experimento. Teniendo en cuenta que el G_1 corresponde a usuarios que pueden considerarse de alta autenticidad (ya que la distancia entre los puntos escogidos en las fases de registro y autenticación son muy pequeñas), el objetivo del experimento es comprobar que el estadígrafo

L-JSB obtenido mediante la transformación JSB del epígrafe anterior es capaz de reconocer con baja probabilidad de error a los usuarios de este grupo.

Grupos de contraseñas. Se definieron 3 grupos de usuarios. G_1, G_2 y G_5. Los grupos G_1 y G_2 son los mismos empleados en [13], pero se definió un nuevo grupo, que se denotara G_5. El grupo G_5 está formado por contraseñas tales que sus 5 puntos están dentro de la región de tolerancia, pero fueron escogidos aleatoriamente dentro de esta región. Se generaron en total 30 000 contraseñas, distribuidas entre los 3 grupos (10 000 contraseñas en cada grupo).

Estadígrafo. Para las contraseñas de cada uno de los 3 grupos anteriores, se calculó el estadígrafo L-JSB, usando los parámetros JSB estimados a partir de la muestra del grupo G_1, a los grupos resultantes los denotaremos como G_{1-2}, G_{2-2} y G_{5-2}. Por la forma de definición, la diferencia entre las contraseñas de G_5 y G_1 debe ser menor que entre G_2 y G_1 y se espera que el estadígrafo transformado L-JSB, refleje ese comportamiento.

Hipótesis. Sean las hipótesis:

H_0 : El usuario es del G_1.

H_1 : El usuario no es del G_1.

Para decidir, con nivel de significación alfa prefijado si una contraseña corresponde o no a un usuario del G_1, se empleará el valor estadígrafo L-JSB asociado a esa contraseña.

Transformación de las Hipótesis. Sea X el valor observado del estadígrafo del modelo L. Teniendo en cuenta que si se aplica a X la transformación de Johnson SB con los parámetros de G_1, entonces se obtiene el valor Z tal que bajo la hipótesis H_0, corresponde a una distribución Normal $N(0,1)$. Las hipótesis anteriores quedan:

H_0 : Z Distribuye $N(0,1)$.

H_1 : Z No Distribuye $N(0,1)$.

Para los grupos G2, G5 se espera (por su forma de definición) que la media $\mu > 0$ y queda una prueba de hipótesis de una cola (cola derecha) para la media de una distribución Normal. Las hipótesis quedarían:

H_0 : $\mu = 0$.

H_1 : $\mu > 0$.

Criterio de decisión. Se seleccionara el nivel de significación $\alpha = 0{,}05$ y la región crítica usual de rechazo de H_0 para la prueba de hipótesis de la cola derecha, para la media de una distribución Normal, la que se muestra en la figura 9.

Alternativamente, si $P - valor(z) < \alpha = 0{,}05$, se rechaza la hipótesis H_0.

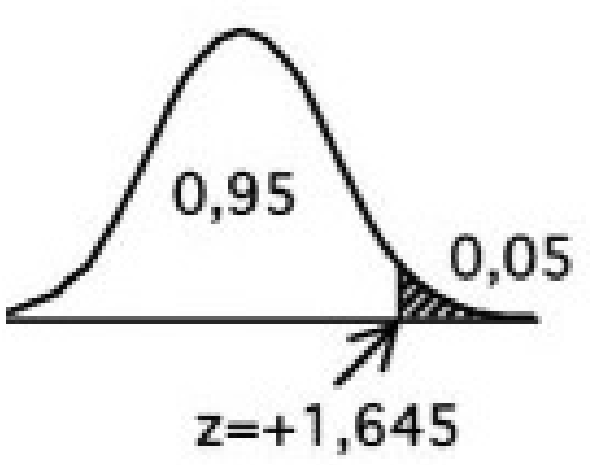

Figura 9. Región crítica (cola derecha) para la media de una distribución $N(0,1)$ para $\alpha = 0{,}05$

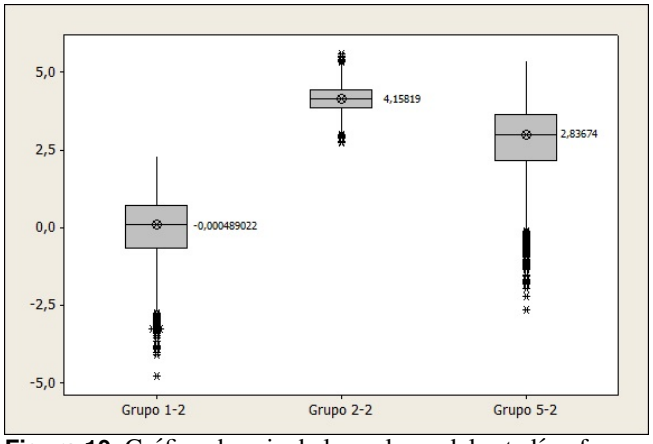

Figura 10. Gráfico de caja de los valores del estadígrafo transformado L-JSB, de los 3 grupos G_{1-2}, G_{2-2} y G_{5-2}

2.2.3 Resultados y discusión del Experimento 2

En la figura 10, se muestra el gráfico de caja-bigote y en la figura 11 los histogramas de los valores del estadígrafo transformado L-JSB en cada uno de los 3 grupos G_{1-2}, G_{2-2} y G_{5-2}.

Discusión de los resultados. En la figura 10 se aprecia que los valores de la media se comportan en orden creciente: $\mu(G_{2-2}) = 4{,}15818 > \mu(G_{5-2}) = 2{,}83674 > \mu(G_{1-2}) = -0{,}000049 \approx 0$, como se esperaba.

Por otra parte, en la figura 11 se aprecia la distribución aproximadamente normal de los tres grupos, aunque en el grupo G_{2-2} se observa mayor simetría, mientas en G_{5-2} y G_{1-2} la cola izquierda es ligeramente más larga que la cola derecha.

Mientras los histogramas de G_{1-2} y G_{2-2} no se interceptan, las colas derechas de G_{1-2} e izquierda de G_{5-2} si se interceptan, esto sugiere que para distinguir entre los grupos G_{1-2} y G_{5-2} el número de decisiones erróneas será mayor que en el caso G_{1-2} y G_{2-2}.

En el grupo G_{2-2} el menor valor observado es 2,8 que es

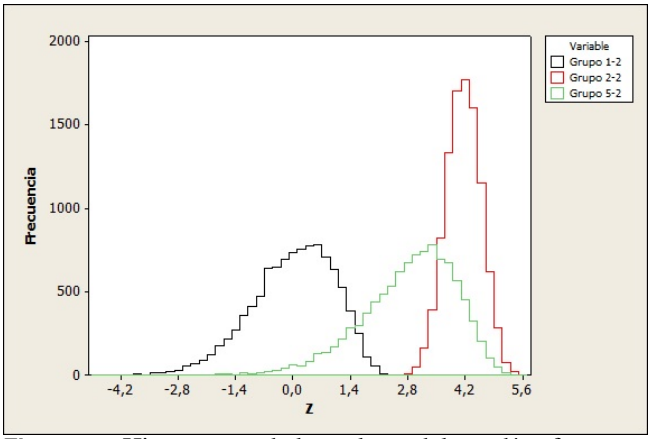

Figura 11. Histogramas de los valores del estadígrafo transformado L-JSB, de los 3 grupos G_{1-2}, G_{2-2} y G_{5-2}

mayor que el valor critico 1,645 fijado por lo cual se debe rechazar en todos los casos su pertenencia a G_{1-2}. En G_{5-2}, hay una parte de las contraseñas tales que el valor de su estadígrafo cae en la región de aceptación de H_0, por tanto, se cometen inevitablemente errores de decisión.

Para cuantificar la magnitud de estos errores se aplicó el test a los 3 grupos.

Aplicación del test en los 3 grupos G_{1-2}, G_{2-2} y G_{5-2}. Los resultados de la aplicación del test a los 3 grupos G_{1-2}, G_{2-2} y G_{5-2}, en una muestra de $n = 10000$ contraseñas en cada grupo se muestran a continuación en los cuadros 3 y 4:

Decisión	G_{1-2}	G_{2-2}	G_{5-2}
No Rechazar H_0 ($z \leq 1{,}645$)	9786	0	1469
Rechazar H_0 ($z > 1{,}645$)	214	10000	8531

Cuadro 3. Número de rechazos de H_0(pertenencia al grupo G_{1-2}) en $n = 1000$ aplicaciones del test L-JSB en cada uno de los 3 grupos, con $\alpha = 0{,}05$.

	G_{1-2}	G_{2-2}	G_{5-2}
No Rechazar H_0 ($z \leq 1{,}645$)	0,9786	0	0,1469
Rechazar H_0 ($z > 1{,}645$)	0,0214	1	0,8531

Cuadro 4. Proporción de rechazos de H_0(pertenencia al grupo G_{1-2}) en $n = 1000$ aplicaciones del test L-JSB en cada uno de los 3 grupos, con $\alpha = 0{,}05$.

A partir del cuadro 4 se puede estimar la probabilidad de cometer un error de tipo I o II en este escenario cuando se emplea el estimador L-JSB, pues $\widehat{P}(\text{Rechazar } G_{1-2}/G_{1-2}) = 0{,}0214$, mientras que para los errores de tipo dos se tiene que $\widehat{P}(\text{No Rechazar } G_{1-2}/G_{2-2}) = 0$ y $\widehat{P}(\text{No Rechazar } G_{1-2}/G_{5-2}) = 0{,}1469$. Estos errores son razonables e ilustran con claridad la ventaja aportada por el estimador L-JSB sobre el estimador L, pues L-JSB permite fijar el valor crítico a partir de la distribución normal y el α prefijado, lo cual representa la mejora y aporte principal de este trabajo para mejorar el estadígrafo del modelo L.

3. Conclusiones

El estadígrafo L propuesto en trabajos previos tiene la ventaja de medir el nivel de autenticidad del usuario, pero la desventaja de que su distribución era desconocida y para su aplicación práctica se requería en cada caso, fijar los umbrales por simulación.

El aporte principal de este trabajo consiste en determinar la distribución del estadígrafo L. Se demostró mediante las pruebas de bondad de ajuste Kolmogorov Smirnov, Anderson Darling y Chi-Cuadrado que las muestras de este estadígrafo L se ajustan a la distribución Johnson SB. Se aplicó la transformación JSB y se confirmó que el nuevo estadígrafo obtenido L-JSB comete pocos errores al distinguir un usuario muy legítimo, como los del grupo G_{1-2}, de otros usuarios menos legítimos, como los del grupo G_{5-2}. Este resultado facilita la aplicación práctica del estadígrafo L y constituye un perfeccionamiento del modelo que le dio origen.

Como problema abierto, se propone investigar el comportamiento del estadígrafo L-JSB en muestras reales de usuarios legítimos y también en muestras de usuarios autenticados mediante ataques de diccionarios, con el objetivo de comparar sus valores y decidir si es capaz de detectar la ocurrencia de un ataque de diccionario autenticado.

Agradecimientos

Se agradece al Instituto de Criptografía y a la facultad de MATCOM de la Universidad de La Habana, por la aprobación y desarrollo del Proyecto "Autenticación Gráfica", dentro del cual se desarrolló esta investigación.

Referencias

[1] O. V. Rodríguez, C. M. Legón, and R. Ll. Socorro. Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica. *Revista Cubana de Ciencias Informáticas*, 12:13–27, 2018.

[2] D. Comaniciu and P. Meer. Mean shift: A robust approach toward feature space analysis. *IEEE Transactions on pattern analysis and machine intelligence*, 24(5):603–619, 2002.

[3] E. B. Borrego, P. E. S. Navarro, and C. M. Legón. Debilidades de los métodos de discretización para contraseñas gráficas. *IV Seminario Científico Nacional de Criptografía. Universidad de la Habana.*, 2018.

[4] O. V. Rodríguez, C. M. Legón, R. LL. Socorro, and P. E. S. Navarro. Patrones en el orden de los clics y su influencia en la debilidad de las claves en la técnica de autenticacion gráfica passpoints. *IV Seminario Científico Nacional de Criptografía*, 2018.

[5] O. V. Rodríguez. Algoritmo para la detección de contrasenas gráficas con patrón de suavidad en la técnica de autenticación gráfica passpoints. Master's thesis, Universidad de la Habana, 2019.

[6] C. M. Legón, R. Ll. Socorro, P. E. S. Navarro, O. V. Rodríguez, and E. B. Borrego. Nuevo modelo probabilístico en autenticación gráfica. *Ingeniería Electrónica, Automática y Comunicaciones*, 40(3):92–104, 2019.

[7] G. E. Blonder. Graphical password, September 24 1996. US Patent 5,559,961.

[8] J. P. Bhootwala and P. H. Bhathawala. Graphical password authentication - survey. *Global Journal For Research Analysis*, 9(2), 2020.

[9] A. Rao. Cyber security - a new secured password generation algorithm with graphical authentication and alphanumeric passwords along with encryption. Master's thesis, Old Dominion University, 2019.

[10] J-C. Birget, D. Hong, and N. Memon. Graphical passwords based on robust discretization. *IEEE Transactions on Information Forensics and Security*, 1(3):395–399, 2006.

[11] S. Chiasson, J. Srinivasan, R. Biddle, and P. C. van Oorschot. Centered discretization with application to graphical passwords. In *UPSEC*. Citeseer, 2008.

[12] K. Bicakci. Optimal discretization for high-entropy graphical passwords. In *2008 23rd International Symposium on Computer and Information Sciences*, pages 1–6. IEEE, 2008.

[13] C. M. Legón. Nuevo modelo probabilístico en autenticación gráfica para medir la autenticidad del usuario. Master's thesis, Universidad de La Habana, 2019.

[14] Mathwave. Easyfit. urlhttp://www.mathwave.com/.

Anexos

Anexo No.1: Bondad de ajuste de la muestra del estadígrafo L en el G_1 con las 6 distribuciones a las que mejor se ajusta la muestra.

Johnson SB					
Kolmogorov-Smirnov					
Tamaño de la muestra Estadística Valor P Rango	1000 0.02129 0.74667 2				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	0.03393	0.03867	0.04294	0.048	0.05151
Rechazar?	No	No	No	No	No
Anderson-Darling					
Tamaño de la muestra Estadística Rango	1000 0.32635 3				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	1.3749	1.9286	2.5018	3.2892	3.9074
Rechazar?	No	No	No	No	No
Chi-cuadrado					
Grados de libertad Estadística Valor P Rango	9 5.124 0.82337 1				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	12.242	14.684	16.919	19.679	21.666
Rechazar?	No	No	No	No	No

Figura 12. Bondad de ajuste de la muestra con la distribución Johnson SB

Kumaraswamy					
Kolmogorov-Smirnov					
Tamaño de la muestra Estadística Valor P Rango	1000 0.02209 0.70488 3				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	0.03393	0.03867	0.04294	0.048	0.05151
Rechazar?	No	No	No	No	No
Anderson-Darling					
Tamaño de la muestra Estadística Rango	1000 0.34584 4				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	1.3749	1.9286	2.5018	3.2892	3.9074
Rechazar?	No	No	No	No	No
Chi-cuadrado					
Grados de libertad Estadística Valor P Rango	9 6.0163 0.73829 2				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	12.242	14.684	16.919	19.679	21.666
Rechazar?	No	No	No	No	No

Figura 13. Bondad de ajuste de la muestra con la distribución Kumaraswamy

Weibull (3P)					
Kolmogorov-Smirnov					
Tamaño de la muestra Estadística Valor P Rango	1000 0.025 0.551 5				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	0.03393	0.03867	0.04294	0.048	0.05151
Rechazar?	No	No	No	No	No
Anderson-Darling					
Tamaño de la muestra Estadística Rango	1000 0.7193 5				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	1.3749	1.9286	2.5018	3.2892	3.9074
Rechazar?	No	No	No	No	No
Chi-cuadrado					
Grados de libertad Estadística Valor P Rango	9 6.766 0.66147 3				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	12.242	14.684	16.919	19.679	21.666
Rechazar?	No	No	No	No	No

Figura 14. Bondad de ajuste de la muestra con la distribución Weibull 3P

Weibull					
Kolmogorov-Smirnov					
Tamaño de la muestra Estadística Valor P Rango	1000 0.02756 0.42585 6				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	0.03393	0.03867	0.04294	0.048	0.05151
Rechazar?	No	No	No	No	No
Anderson-Darling					
Tamaño de la muestra Estadística Rango	1000 0.8091 6				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	1.3749	1.9286	2.5018	3.2892	3.9074
Rechazar?	No	No	No	No	No
Chi-cuadrado					
Grados de libertad Estadística Valor P Rango	9 11.296 0.25596 5				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	12.242	14.684	16.919	19.679	21.666
Rechazar?	No	No	No	No	No

Figura 15. Bondad de ajuste de la muestra con la distribución Weibull

Gen. Extreme Value					
Kolmogorov-Smirnov					
Tamaño de la muestra Estadística Valor P Rango	1000 0.01891 0.85998 1				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	0.03393	0.03867	0.04294	0.048	0.05151
Rechazar?	No	No	No	No	No
Anderson-Darling					
Tamaño de la muestra Estadística Rango	1000 16.168 31				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	1.3749	1.9286	2.5018	3.2892	3.9074
Rechazar?	Sí	Sí	Sí	Sí	Sí

Figura 16. Bondad de ajuste de la muestra con la distribución Gen Extreme Value

Beta					
Kolmogorov-Smirnov					
Tamaño de la muestra Estadística Valor P Rango	1000 0.02445 0.57985 4				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	0.03393	0.03867	0.04294	0.048	0.05151
Rechazar?	No	No	No	No	No
Anderson-Darling					
Tamaño de la muestra Estadística Rango	1000 2.7882 7				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	1.3749	1.9286	2.5018	3.2892	3.9074
Rechazar?	Sí	Sí	Sí	No	No
Chi-cuadrado					
Grados de libertad Estadística Valor P Rango	9 11.22 0.26093 4				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	12.242	14.684	16.919	19.679	21.666
Rechazar?	No	No	No	No	No

Figura 17. Bondad de ajuste de la muestra con la distribución Beta