Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online)
Volume 30, Issue 1, 2019
DOI: http://doi.org/10.23851/mjs.v30i1.421

Research Article **Open Access**

User Authentication Secure by Randomly Cubic Spline Curve and Blum Blum Shub Algorithm

Hanaa Mohsin[1*], Ahmed Oday[2]
[1] Department of Software, Computer Science, University of Technology, IRAQ
[2] Department of Information Security, Computer Science, University of Technology, IRAQ
*Correspondent author email: salmanhanna2007@yahoo.com

ArticleInfo

Received
23/12/2017

Accepted
19/08/2018

Published
15/08/2019

Abstract

With the tremendous development witnessed by the world in recent times, computer security significance expanded as insurance procedure of registering systems and authentication the user with scientific and technological developments are increasing every day. This assurance procedure is connected for touchy information such of electronic business, electronic learning, and electronic saving money exchange, online networking and more administrations over the web by utilizing login application to distinguish the character for doing this authentication. The problem of user authentication and experimental data collection to detect user with speed process without confuses. This paper solve this problem by used Cubic Spline to easy represented name and easy detected by distance Euclidean equation, authentication techniques utilized as insurance process by securing name mix with Blum Blum Shub (BBS) algorithm that have randomly number. In this work, the application is founded on type name that the combine with BBS and represented by cubic spline. The results of proposed work generate randomly number to drawing the curve to detect and the rate of different shape in cubic spline curve that can be detected. Assurance gives affirmation distinguished suitable security and easy way to complicate security applications.

Keywords: Detect User Authentication, Cubic Spline Curve, Virtual Keyboard, Blum Blum Shub.

الخلاصة

مع التطور الهائل الذي شهده العالم في الآونة الأخيرة، توسعت اهمية حماية الكمبيوتر كإجراء تأمين لأنظمة التسجيل والمصادقة للمستخدمين مع التطورات العلمية والتكنولوجيا آخذت في التزايد كل يوم. إجراءات الضمان ترتبط بمعلومات حساسة مثل هذه الأعمال التجارية الإلكترونية، والتعلم الإلكتروني، وتداول النقود الإلكترونية، والتواصل عبر الإنترنت، والمزيد من الإدارات عبر الويب من خلال استخدام تطبيق تسجيل الدخول لتمييز الشخصية التي تقوم بالمصادقة. مشكلة مصادقة المستخدم وعمليات جمع البيانات للكشف عن المستخدم مع سرعة في العمل بدون خطاء. هذه البحث يحل هذه المشكلة عن طريق استخدام منحني مكعبي إلى الاسم لسهولة تمثيله وسهولة الكشف عن طريق المعادلة الإقليدية ، وتقنيات المصادقة المستخدمة كعملية تأمين من خلال تأمين مزيج الاسم مع خوارزمية (Blum Blum Shub BBS) التي تحتوي على رقم عشوائي. في هذا العمل ، تم تأسيس التطبيق على اسم النوع الذي يتم دمجه مع (BBS) وتمثله بمنحني مكعبي. النتائج العمل المقترح تولد رقمًا عشوائيًا لرسم المنحنى لتميز نسبة اختلاف الاشكل في منحني مكعبي الذي يمكن تميزه. ضمان الحماية يمنح تأكيدا تميز مناسباً وتعتبر طريقة سهلة لتعقيد التطبيقات الأمنية.

Introduction

A pseudo-random sequence generator (PRNGs) is an algorithm that allows the generation of long bit sequences and more complicated than small initialization values [1][2]. However, for authentication and encryption assignments, in addition, breezing through standard measurable tests, pseudo-random sequences should be unpredictable for real computers. Protection of a pseudorandom generator is a particular that shows that it is so difficult to difference between the pseudorandom sequences (PRS) and really random sequences (RRS). For the BBS pseudorandom generators acknowledge these two apportionments is as difficult as study a huge composite number [3]. The protection of BBS generator is completely construe has been ambiguous how to follow the

parameter and the size number of bits that output on each repetition, a required level of security is come to, while limiting the computational per output bit [4].

Related Work

In 2012 [2]: The security of the BBS as PRNGs is fundament on integers modulo that are properties of mathematical. Some fundament concept of number hypothesis: an number is a quadratic buildup it is identical to a square modulo m. Jacobi number was an number modulo m is the result of each prime agent of m. Legendre number of an number (modulo a prime *h* number) is +1 if it is a square residue, and −1 otherwise. BBS contribution the square residuosity issue, the issue of choosing for Z*m (the multiplicative group of integers modulo m), where m is the result of two distinct odd primes, whether elements with Jacobi +1.

In 2015 [6]: (PRNGs) are sensitive number Primitives that used widely and with more applications such as password, numerical simulations or protection. They are one of cryptosystem has to embed of the fundamental computer component for cryptosystem, for key streams in symmetric ciphers or key generation ciphers. The PRNGs must accomplish prerequisites as security, statistical quality, speed and soon. The Field Programmable Gate Arrays (FPGAs) have been powerfully utilized for knowing the speed prerequisite in (PRNGs), two methods was their high parallelization capability. Advantages are very useful and cost the way of performance, flexibility, design time, consumption, power and cost.

In 2016 [5]: explain by use chaotic map dynamical order as PRNGs, between more things such the systems. Their sensitivity to initial conditions that was unpredictability, the secure and random by broadband spectrum product is a good candidate to generate sequences. For instance, strengthen optical communications, can product by chaos-based generators that was a good used.

In 2017 [1]: changing the input parameters of the algorithm, it is possible to adjust the key generation time and thereby to adapt the proposed algorithm to specific authentication and encryption tasks.

Materials and Methods

Blum Blum Shub Pseudo-Random Sequence Generator

A PRNG is algorithm generate a sequence real binary number of length L as a deterministic with the randomly number, result is an number 0,1 sequence of length m > L that mean is a binary sequence "looks random sequence". The Algorithm BBS need the input to generator that which call seed and the results of algorithm which is called the pseudorandom bit sequence. Protection a pseudorandom generator is a distinguishing that appear to the Repetition distinction between the arrangements pseudorandom and genuine irregular successions. BBS pseudorandom generator acknowledgment the two successions are as troublesome as figuring a gigantic composite number.

The BBS PRNGs is the following Steps:

- Generate A and B, as two great Blum prime numbers.
- M = A • B.
- Select C2 [1, M − 1], the random seed.
- Y_0 = C2 mod M.
- The sequence is defined as $Y_i = Y_{2i}-1$ mod M and S_i = parity(Y_i).
- The Result is S_1, S_2, S_3, ... where parity(Y_i) is 0 when Y_i is even and 1 when Y_i is odd.

Cubic Spline curve

A spline is the points (a_k,b_k) for k = 0, 1, ..., m. in actual individual curved that is created from a put of piecewise uninterrupted, a outputs of interpolation activity sk(a) for k=1,...,m−1. A spline curve create from 4part of rule, to more explain we have 5 interpolating as example, dot it likes a single part of smooth curve[7]. This is get, as the spline is continuous at all joints. The spline is likewise ceaseless in from derivatives equation at these points that spoke to at the smoothness bends. A spline of grade n is produce from piecewise polynomials of a similar degree [8]. A quadratic spline comprises of quadratic polynomials connecting the points. The simplest spline is direct streak join with points continuous, which mean that

consist it. The cubic spline is the curve has the principle trait that join the points through cubic polynomials, equation it is differentiable in its first and second derivatives is join point between any 2 parts of function. Figure 1 represent a cubic spline interpolated over 4 points (a_k,b_k), for k = 0, 1, 2, 3, whose part are indicate as sk(a) for
k =1,2,3. Each part of the spline is a continuous cubic function in the given sub period. The spline show to be very smooth at each inward node as its first and second derivatives point [9].

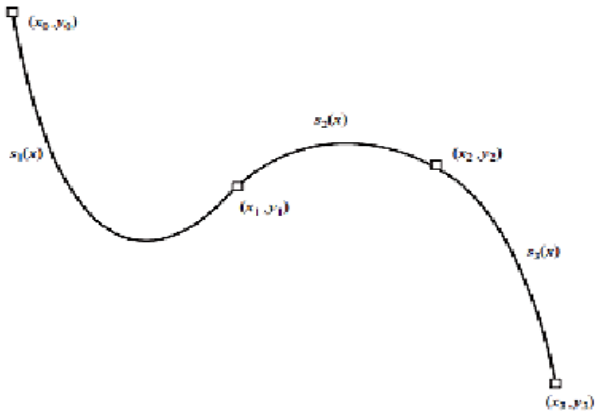

Figure 1: A Cubic spline interpolated from four points.

Proposed System

Run the BBS algorithm by the p=11, q= 19, seed =13, and 30 random number. Output is = {169 137 168 9 81 82 36 42 92 104 157 196 169 137 168 9 81 82 36 42 92 104 157 196 169 137 168 9 81 82}. These the 30 random number will have used for summation with the index in matrix (x,y) as (12,11), is used full high random index matrix that give the wide range in cubic spline interpolation. By Matlab 2017 was run the algorithm.

Virtual Keyboard as a Matrix

A virtual Keyboard letter is instant as matrix, which include row and column that have letter sorted by any type as Figure 2, below are the principal track for produce virtual keyboard:
Step1: produce matrix that size (12×11), 12 rows and 11 columns that cells have all probability of key press the description of the language such as Arabic, English and the special describe "all properties of ASCOII", number and these size is a improve size about redundancy.
Step 2: The benefit of this matrix letter virtual keyboard is to convert the character from one value representing in a computer ASCOII to a value consisting of (x, y) that's mean the characters are represented as point (x, y) tow value represented the characters such as coding letter.
Step 3: take name as sequence of letter set as A
1- Cut every set of A as one characters.
2- Searcher in matrix letter of the character.
3- After found the character in matrix take the value of the cell, that mean the value of row and column, and save these values as a vector to represents that character.
4- Repeated the (1, 2, 3) steps for each character and saved the value in vector of two value (row and column) for each character. The steps to programming of convert the name to point as two values (see Algorithm 1. The sequence of letter in matrix can be change and sorted by what you wanted to sort such as (every letter capital and small, or all capital after all small, etc) in Figure 3.

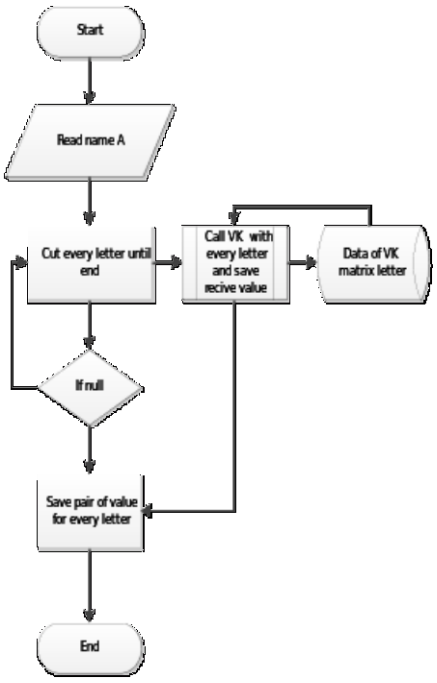

Figure 2: Flowchart of convert name to points.

	1	2	3	4	5	6	7	8	9	10	11
1	a	b	c	d	e	f	g	h	i	j	ض
2	k	l	m	n	o	p	q	r	s	t	ص
3	u	v	w	x	y	z	A	B	C	D	ث
4	E	F	G	H	I	J	K	L	M	N	ق
5	O	P	Q	R	S	T	U	V	W	X	ف
6	Y	Z	0	1	2	3	4	5	6	7	غ
7	8	9	!	@	#	$	%	^	&	*	ع
8	(	)	_	-	=	+	\	?	.	>	ه
9	[	]	;	,	<	"	:	/	~	}	خ
10	{	|	ش	س	ب	ل	ا	ت	ن	د	ح
11	م	ك	ط	ظ	ز	و	ة	ى	لا	ر	ج

Figure 3: Matrix contain letter as tow dimension.

Algorithm 1: Convert Name to points.

Input: a) user name A, b) matrix of letter M.
Output : (x,y) point for ever character

```
Begin
  Step 1:- set char (k) = cut every character from A
Step 2 :- set M matrix (12,11) =that content characters
Step 3:- For i=0,…,12
          For j=0,…,11
              If char (k)=matrix (I,j) then
                  Xk =i
                  Yk=j
              End if
           Next
          Next
End
```

Create Cubic Spline Curve

Now the step how to convert the name from letter to cubic curve

Step 1: In previse phase known about how convert name to two value, now after convert take every pairs of value and separated as a point(x,y), that mean every pair as point from x-axis, y-axis.

Step 2: every X value from all point was put in group set as Xp also that would do for Y value, put in group set as Yp.

Step 3: Xp, Yp, was the input excellence for the cubic Spline curve algorithmic rule as a use for drawing spline. The output of the algorithm is simplest curve was describe in Figure (4A) in green curve, the blue line that represented as smooth depiction line; It was the cubic curve that benefit in next phase. Example: the name fawzey is different from the Fawzey with start capital letter because start small letter must start with capital as a Name. Now, enter name and called the matrix phase and cubic phase the point of Fawzey is (173.11), (138, 82), (171.85), (12.42), (82.47), (85.97). The point represented on axes and connected between that, cubic spline algorithm was drawing the smooth curve that represented as blue line in mutiny steps. Create cubic spline phase. Figure 4 shows different example about the represented of name.

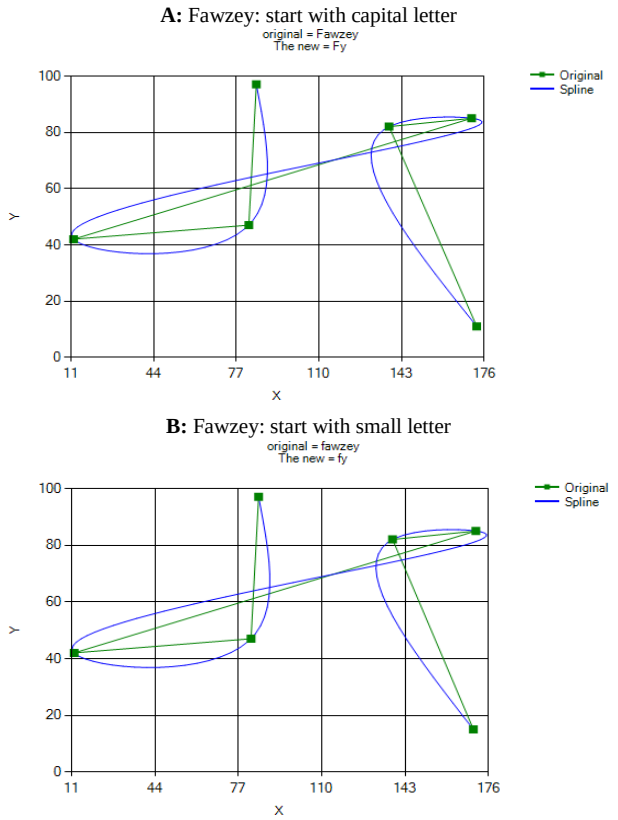

Figure 4: Impact of using or not using capital for name.

Figure 4 shows the same name with different capital letter If not used the randomly value test the curve will not be the high range and will be easy for distinguish by brute force attack. Figure 5 shows the different between used random or without used.

Results and Discussion

The paper verify on the subject level touching appropriate name by Cubic Spline interpolation. The implementation of these technique cubic spline is cheap, cost-effective and not request for special device. The output of this paper is suited by the different attempt user write his name the index of matrix was summation every attempt with new randomly number, these method was useful if duplicated the letter in name or if letter in same row with other letter in these case was letter in row was

not change, solve these problem by BBS randomly, Figure 6.

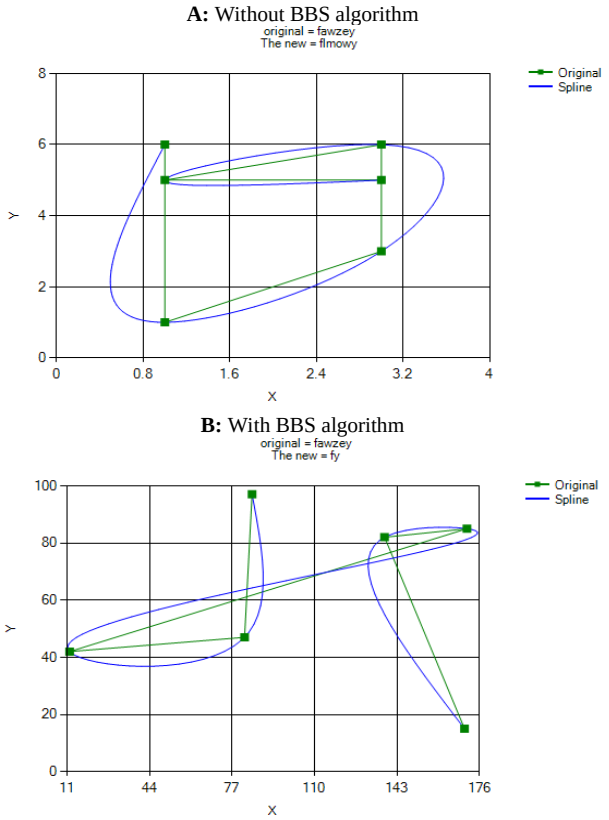

Figure 5: The different with or without BBS algorithm.

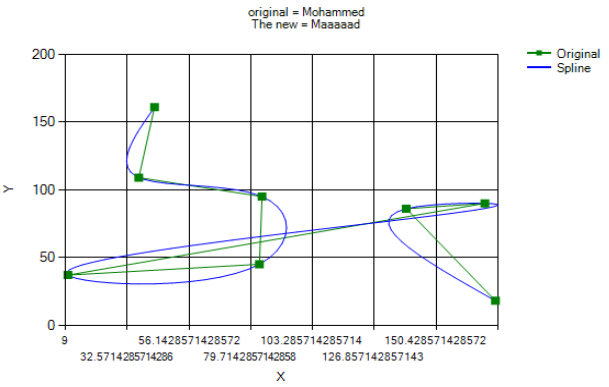

Figure 6: Show the duplicated in letter (m).

Also, Figure 5-A, show the letter a, h, e and d was in same row in Figure 3 the BBS sole these problem. The proposal methods are run in the English, special characters, number and Arabic alphabet. Figure 7 represented all probability of characters. A: the name with English alphabets, B: Arabic alphabet, C: Arabic alphabet with title, the proposal methods can be represented in these cases. D: combine between the English capitol and small letter, Arabic, special and number. The figure (8) show the another user with same name and different last name that give wide different area of cubic spline. This proposed method is generating according to human name behavior typing when name typing with title or complete name give special spline curve to represent the name with different shape. The key in same letter was giving the different way in curve point.

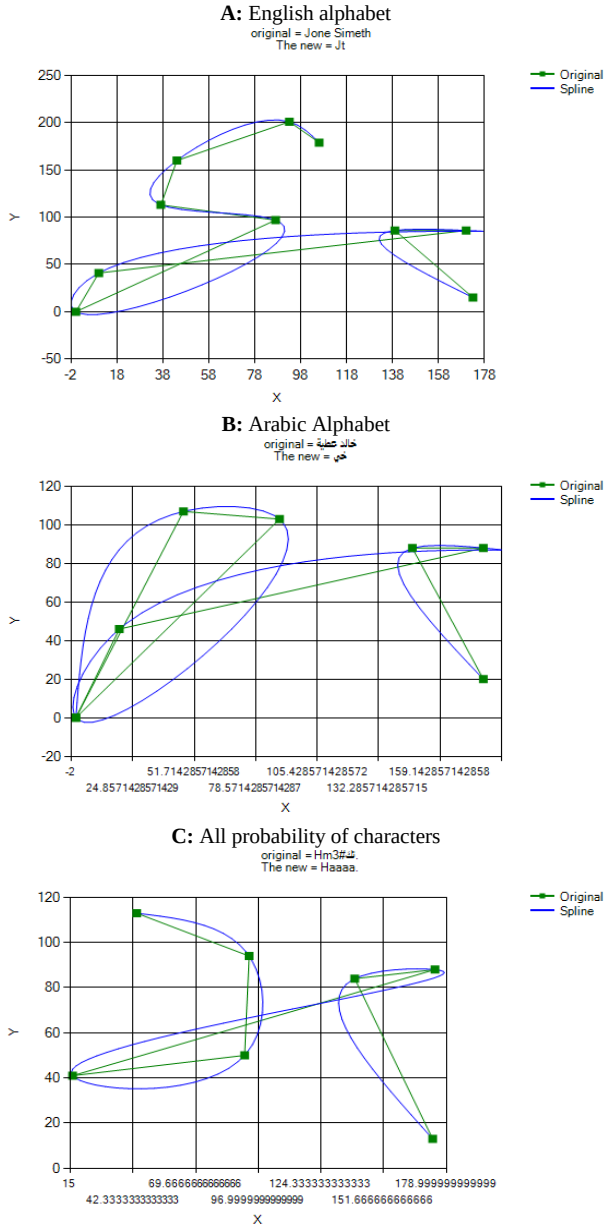

Figure 7: The different curve in all characters.

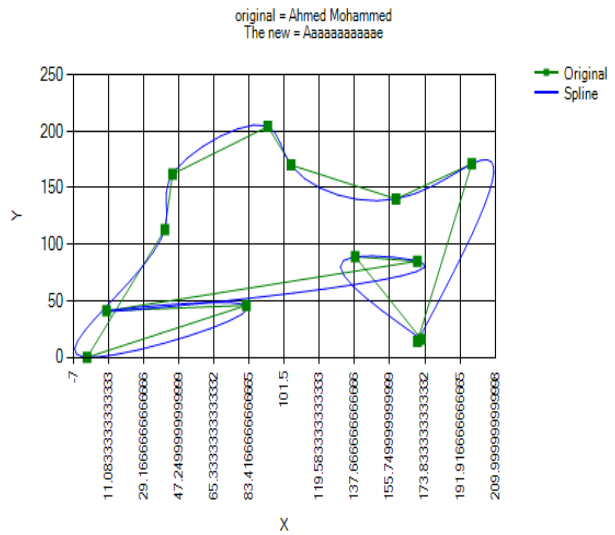

Figure 8: Example of name (Ahmed Mohammed).

Conclusion

This paper is constant to ready authorized users to log in or any application that utility his name by using VK, BBS, and Cubic spline interpolation. The range change in index finger of Output VK in the change of the output modern curve, the Virtual-Keyboard is safe factor Hardware, software system from attack. Changing the input in every attempt, the output changes the modern curve. The way of change sorted input in letter matrix is a utility for the proposed methods in work for exactly authorized the user. The changes indicate for every name for each user can generate the modern curve with many smooth curves. For forward work, suggest being more secure authentication system by supported by some features of writing name, Develop the algorithm for complex randomly in sorted matrix, these useful in performance accuracy of the system. Also by move the situation of original line by point that will drawing a different cubic spline curve with amazing shape by many methods.

Reference

[1] Y. D. Vybornova, "Password-based key derivation function as one of Blum-Blum-Shub pseudo-random generator applications," Procedia Eng., vol. 201, pp. 428–435, 2017.

[2] R. Affeldt, D. Nowak, and K. Yamada, "Certifying assembly with formal security proofs: The case of BBS," Sci. Comput. Program., vol. 77, no. 10–11, pp. 1058–1074, 2012.

[3] Salil P. Vadhan, "Pseudorandom generators," in Motivation and Definitio, Theoretica., no. November, vol. 24, pp. 213, 2012.

[4] Mikael Olsson Niklas ullberg, "Blum Blum Shub on the GPU A performance comparison between a CPU bound and a GPU bound Blum Blum Shub generator," Blekinge Institute of Technology, vol. 83, pp.17–25, 2012.

[5] J. Lee, "Establishing a case for improved food phenolic analysis.," Food Sci. Nutr., vol. 2, no. 1, pp. 1–8, Jan. 2014.

[6] X. Fang, Q. Wang, C. Guyeux, and J. M. Bahi, "FPGA acceleration of a pseudorandom number generator based on chaotic iterations.," J. Inf. Sec. Appl., vol. 19, no. 1, pp. 78–87, 2014.

[7] L. László, "Cubic spline interpolation with quasiminimal B-spline coefficients," Acta Math. Hungarica, vol. 107, no. 1–2, pp. 77–87, 2005.

[8] Y. Nievergelt, "Splines in Single and Multivariable Calculus," COMAP, vol. 2420, no. 617, 1993.

[9] S. Salleh, A. Y. Zomaya, and S. A. Bakar, "Computing for Numerical Methods using Visual C ++," vol. 34, no. 6, pp. 30–31, 2009.