University of Baghdad
College of Engineering
JE
JOURNAL OF ENGINEERING

Journal of Engineering

journal homepage: www.joe.uobaghdad.edu.iq

Volume 29 Number 6 June 2023

A Modified Vigenère Cipher based on Time and Biometrics features

Bashar Adel Esttaifan
Department of Electronic and Communications, College of Engineering, University of Baghdad, Baghdad-Iraq
bashar.s@coeng.uobaghdad.edu.iq

Abstract

Biometrics is widely used with security systems nowadays; each biometric modality can be useful and has distinctive properties that provide uniqueness and ambiguity for security systems especially in communication and network technologies. This paper is about using biometric features of fingerprint, which is called (minutiae) to cipher a text message and ensure safe arrival of data at receiver end. The classical cryptosystems (Caesar, Vigenère, etc.) became obsolete methods for encryption because of the high-performance machines which focusing on repetition of the key in their attacks to break the cipher. Several Researchers of cryptography give efforts to modify and develop Vigenère cipher by enhancing its weaknesses. The proposed method uses local feature of fingerprint represented by minutiae positions to overcome the problem of repeated key to perform encryption and decryption of a text message, where, the message will be ciphered by a modified Vigenère method. Unlike the old usual method, the key constructed from fingerprint minutiae depend on instantaneous date and time of ciphertext generation. The Vigenère table consist of 95 elements: case sensitive letters, numbers, symbols and punctuation. The simulation results (with MATLAB 2021b) show that the original message cannot be reconstructed without the presence of the key which is a function of the date and time of generation. Where 720 different keys can be generated per day which mean 1440 distinct ciphertexts can be obtained for the same message daily.

Keywords: Security, Minutiae, Vigenère, Caesar, Encryption, Ciphering and Fingerprint.

*Corresponding author
Peer review under the responsibility of University of Baghdad.
https://doi.org/10.31026/j.eng.2023.06.10
This is an open access article under the CC BY 4 license (http://creativecommons.org/licenses/by/4.0/).
Article received: 21/09/2022
Article accepted: 01/11/2022
Article published: 01/06/2023

تشفير فيجينر المعدل بالاعتماد على الوقت والمقاييس الحيوية

بشار عادل اسطيفان
قسم الهندسة الالكترونية والاتصالات – كلية الهندسة – جامعة بغداد

الخلاصة

تُستعمل القياسات الحيوية على نطاقٍ واسع مع أنظمةِ الأمان في الوقت الحاضر؛ فلكل طريقة بيومترية فوائدٌ وخصائص تميزها، فهي تُوفر التفرد والغموض لأنظمة الأمن. يتناول هذا البحث استعمال ميزات القياسات الحيوية لبصماتِ الأصابع، والتي تسمى (التفاصيل الدقيقة) لتشفير رسالة نصية وضمان الوصول الآمن للبيانات في الطرف المستلم للرسالة. يتناول البحث استعمال السمات الحيوية لبصمة الإصبع، والتي تسمى (التفاصيل الدقيقة) لتشفير رسالة نصية وضمان وصول البيانات بأمان إلى طرف المستلم. أصبحت أنظمة التشفير الكلاسيكية (Caesar, Vigenère، إلخ) طرقاً قديمة للتشفير بسبب الحواسيب عالية الأداء التي استُعملت في الهجوم والتي تركز على تكرار مفتاح التشفير لكسره. يبذل العديد من الباحثين في علم التشفير جهودًا لتعديل وتطوير تشفير Vigenère من خلال تعزيز نقاط ضعفها. تستخدم الطريقة المقترحة ميزة محلية لبصمة الإصبع ممثلة بمواضع التفاصيل الدقيقة للتغلب على مشكلة المفتاح المتكرر لأداء تشفير وفك تشفير رسالة نصية، حيث سيتم تشفير الرسالة بواسطة طريقة Vigenère معدلة. على عكس الطريقة المعتادة القديمة، يعتمد المفتاح الذي تم إنشاؤه من تفاصيل بصمة الإصبع على التاريخ الفوري ووقت إنشاء النص المشفر. يتكون جدول Vigenère من 95 عنصرًا: حروف كبيرة وصغيرة وأرقام ورموز وعلامات ترقيم. تظهر نتائج المحاكاة (MATLAB 2021b) أنه لا يمكن استعادة الرسالة الأصلية دون وجود المفتاح الذي يعتمد على تاريخ ووقت توليده. حيث يمكن توليد 720 مفتاحًا مختلفًا يوميًا مما يعني أنه يمكن الحصول على 1440 نصًا مشفرًا مميزًا لنفس الرسالة يوميًا.

الكلمات الرئيسية: الأمنية، تفاصيل بصمة الاصبع، فيجينر، قيصر، التشفير، بصمة الاصبع.

1. INTRODUCTION

During the sixteenth century several shift ciphers were invented. The French mathematician, Blaise de Vigenère suggested one of famous polyalphabetic ciphers that called Vigenère cipher which considered by many involved people to be immune and secure until the twentieth century where two gentlemen, Charles Babbage and Friedrich Kasiski who independently discovered how to break polyalphabetic ciphers including Vigenère. A few decades after Kasiski, William F. Friedman developed an efficient cryptanalytical technique depends on index of coincidence to predict the length of key that led to break these types of cipher **(Trappe and Washington, 2006; Dooley, 2018).** After the computer revolution in the previous century, classical cipher became not familiar to use, because of the huge ability of supercomputer that used by attackers to break these types of ciphering **(Dooley, 2018)**.

In the last decades, communication growth rapidly and the integrity of data transmitted have been achieved by cryptography which became a vital issue; Cryptography experienced unprecedented transition from simple mathematical functions to complicated algorithms that used in encryption and decryption. Various Symmetric and asymmetric cryptographical

systems have been suggested and gained prominence due to the time required to find the key which is important to measure the strength of these algorithms **(Kako et al., 2020; Ibrahim et al., 2021; You et al, 2021).**

Several searchers tried modifying polyalphabetic ciphers (mainly Vigenère technique) to bring it up to date again by various improvements contributions, one of these attempts done by stuffing the original key with pseudo random bits **(Wilson and Garcia, 2006)**. But **(Kester, 2012)** earned a good idea summarized by dynamic changing of the key after each encryption process, however the new key was related to the previous one. Some plaintexts may contain symbols, punctuation and case sensitive English alphabet, thus **(Rahmani et al., 2012)** extends the cipher domain from 26 English alphabets to 92 characters.

A hybrid encryption method for plaintext was introduced by **(Kester, 2013)**. Where the plaintext decrypt based on the columnar transposition cipher, and Vigenère cipher is used to decrypt the plaintext from ciphertext. Finally, the ciphertext was deciphered using cryptanalysis techniques.

A combination between Vigenère and other modern approach such as stream ciphers offers a high level of security, whereas a Vigenère based cipher does not. **(Subandi et al., 2017)** proposed three-pass protocol for the keystream generator of the Vigenère. Also **(Sharif et al., 2018)** enhanced Vigenère through combination with One Time Pad (OTP) algorithm in the three-pass protocol. An algorithm was proposed to generate encryption keys based on discrete wavelet transformation **(Shiltagh et al., 2019). (Uniyal et al., 2020)** proposed an approach to enhance the security of Vigenère by key domain maximization in a finite field. A random main key is used to derive the keys for encryption and decryption processes.

Many key binding and key generation methods were invented to merge biometric with cryptography **(Jegede et al., 2017)**. The most used biometric is Fingerprint due to its unique properties and simplicity of feature extraction **(Angaye et al., 2013)**.

As security ciphering systems, Biometric based systems are exposed to attackers, so that development of biometric algorithms are continuously developing with time proceeding **(Yang et al., 2014)**. A hybrid ciphering method was carried out by doping chaos logistic map with fingerprint features to produce the key of encryption **(Jerjees et al., 2020)**. In the same time of ciphering enhancement, Attacker develop new techniques to break the cipher where Genetic algorithm was used to find the key of encryption, and the essential factor of objective function was the frequency analysis **(Omran et al., 2011), (Salih and Mahmood, 2019).** Recently, deep learning-based Cryptanalysis is under focus, long short-term memory (LSTM) networks tested to break the cipher and the throughput was encourageous to deal with this type of Cryptanalysis **(Ahmadzadeh et al., 2021)**.

The aim of this work is about using fingerprint minutiae and instantaneous time to generate ciphering key that used to encrypt text by modified to ensure safe arrival of data.

2. FINGERPRINT IMAGE ENHANCEMENT

The quality of fingerprint image is a very important factor in fingerprint-based cryptosystems. Many enhancement techniques were invented since the use of biometrics, where bad quality images would affect feature extraction process **(Nedjah et al., 2017)**. The famous classification of fingerprint is the Henry classification **(Henry, 1900)**, which is used significantly in the recognition systems. Two levels of features which are global and local features are used to extract minutiae **(Bhargava et al., 2013)**. The pre-processing and post processing of the fingerprint image are summarized in the **Fig. 1**.

In this paper, the image enhancement of fingerprints (**Fig. 2 (a)** as an example) is performed by enhancing the frequency of the pixels. fingerprint image with dimensions (m×n) split into small images with dimensions (M×N) called blocks then contextual filtering by Fast Fourier transformation is applied. From Eq. (1), $f(x,y)$ is a block and $F(u,v)$ is its FFT as illustrated. **(Willis et al., 2001; Zafer et al., 2014).**

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times \exp\left\{-2j\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \quad (1)$$

where: x=0, 1, 2, …, M-1 and y=0, 1, 2, …, N-1.
(M×N) is the block dimensions which is usually (16×16 or 32×32 pixels).
$F(u,v)$ is the FFT of block with position (u,v).
u=0, 1, 2, …, $(\frac{m}{M}-1)$ and v=0, 1, 2, …, $(\frac{n}{N}-1)$.
and (m×n) is the fingerprint image dimensions in pixels.
Frequency domain enhancement summarized by multiplying the FFT of each block with its magnitude raised to power of *K,* the enhanced image block $g(u,v)$ is in frequency domain as in Eq. (2).

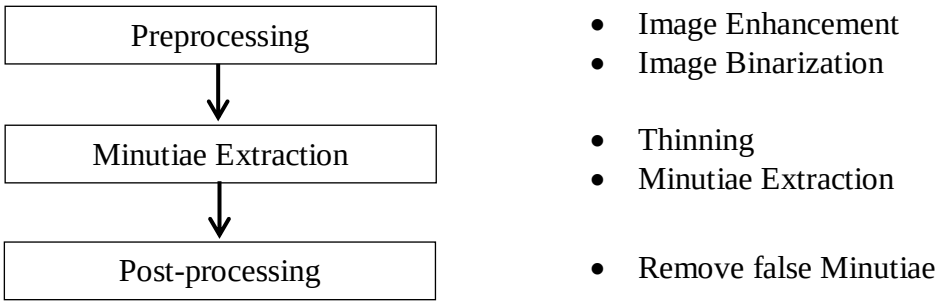


Figure 1. Flow diagram of feature extraction process **(Jerjees et al., 2020)**.

$$g(u,v) = \{F(u,v) \times |F(u,v)|^K\} \quad (2)$$

Where *K* is a variable measured experimentally and the magnitude of each block is given in Eq. (3).

$$magnitude\ of\ FFT = abs\big(F(u,v)\big) \equiv |F(u,v)| \quad (3)$$

IFFT is calculated by Eq. (4) to obtain the enhanced image block $\acute{f}(x,y)$.

$$\acute{f}(x,y) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} g(u,v) * \exp\{2j\pi \times (\frac{ux}{M} + \frac{vy}{N})\} \quad (4)$$

The enhanced image is a function of experimental variable (K). Different values of *K* lead to various minutiae combinations (number and positions) **(Willis et al., 2001)**. **Fig. 2 (b)** is an enhanced version of **Fig. 2 (a)** with *K*=**1.10.** After ridge enhancement, a binarization method is applied to the enhanced image to convert it into binary image then the minutiae may be

specify by thinning and crossing number method **(LS-WL et al., 1992)**. The result of binarization, thinning and minutiae finding are shown in **Fig. 2 (c, d, and e), respectively.**

3. PROPOSED METHOD

Ciphering is a process of protecting important information by encrypting readable message and converts it into unreadable form. The following steps are suggested to cipher a message using modified Vigenère method by a key generated from fingerprint and associated with instantaneous time and date.

a. Get the instantaneous date (xxxx-xx-xx) and time (hh:mm PM or AM)
b. Specify the fingerprint that must be used depending on the date where 365 different fingerprints will be needed per year.
c. Enhance fingerprint image by K (enhancement factor of Eq. (2)) which is proposed to be a function of instantaneous minute (m).
d. Find minutiae (ridges and bifurcations) using crossing number method as in **(LS-WL et al., 1992; Willis et al., 2001; Zafer et al., 2014; Jerjees et al., 2020)**
e. Specify a reference point on the enhanced fingerprint image, for this paper it will be according to the instantaneous hour (h).
f. Find the key by calculating the Euclidian distance between the reference and the other minutiae points.
g. Encode each character of message to corresponding numerical value, this process will be date dependance. This will lead to 365 different encoding schemes.
h. The encryption process is done through adaptive shifting operation (or Adaptive Vigenère) depending on generated key. The AM and PM time yields to positive and negative shifting process respectively.

4. KEY GENERATION FOR THE SUGGESTED METHOD

This method assumed that, the sender and receiver share an information about the time and date of encryption process. Applying the image enhancement of section 2 to the selected fingerprint according the value of K. This paper suggests a relation of K with the instantaneous minute (m) as in Eq. (5).

$$K = \frac{2\times m}{100} + 0.8 \tag{5}$$

where m from 0 to 59 minutes and K will be between 0.8 and 2.0 which is agreed to **(Willis et al., 2001; Zafer et al., 2014; Jerjees et al., 2020).** Therefore, thinning and minutiae extraction were done as in these articles. The list of minutiae positions can be obtained and the Euclidian distance between these minutiae and a reference point will be calculate from Eq. (6).

$$key(n) = \sqrt{(x_n - x_o)^2 + (y_n - y_o)^2} \tag{6}$$

for n=1 to L

where:

L is the key length and represents the number of minutiae points.

x_n and y_n is the position of nth minutiae point.

x_o and y_o is the position of a reference point.

To enhance the security level, the key generation will be time dependent again, where the reference point will select depending on the hour of the encryption process. The key generation is associated with time and date through: the fingerprint which chosen based on date, the enhancement factor (K) carried out by the minutes (m) and the reference points that is depend on the hour (h). Eq. (7) will used to calculate the key which is the Euclidian distance from time-based reference point.

$$key(n) = \sqrt{(x_n - r_o \cos(\frac{\pi h}{6}))^2 + (y_n - r_o \sin(\frac{\pi h}{6}))^2} \quad (7)$$

$r_o$is the radius of the reference cycle where reference point located. $r_o \cos(\frac{\pi h}{6})$ and $r_o \sin(\frac{\pi h}{6})$ is the position of time-based reference point, and h represent the hour of sending.

5. RESULTS AND DISCUSSION

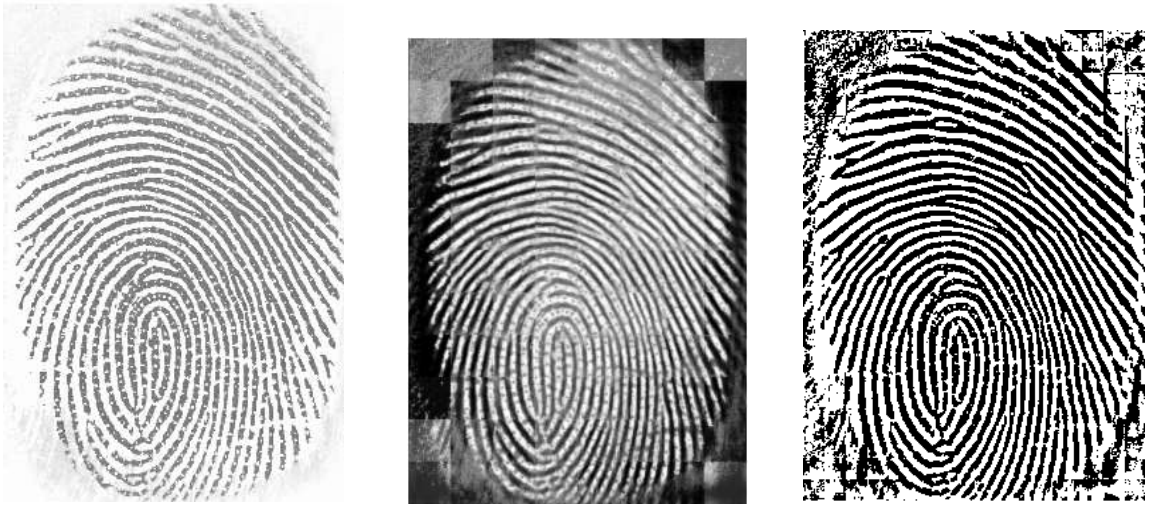
The proposed cryptosystem was simulated using Matlab. The phrase (Ziggurat of Ur) is used as a short message to testify and submit the results clearly. The date of encryption process is assumed to be the first of January, 2022 and the time is (8:15 AM).

The fingerprint image corresponding to the first of January, 2022, is shown in **Fig. 2 (a)**. The image of fingerprint had to pass through many pre-processing and post-processing operations to enhance the image quality in order to get minutiae points as shown in **Fig. 2 (b, c, d and e)**. K is equal to (1.10) by substitute m=15 minutes in Eq. (5).

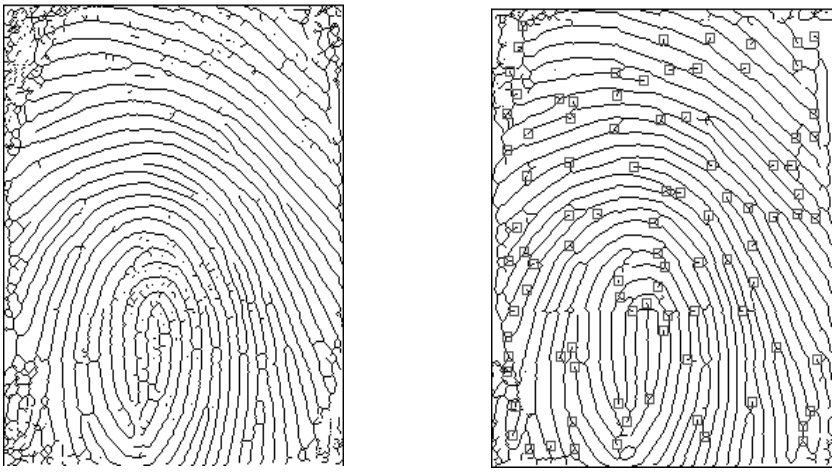
The reference point (x_o, y_o) will be (33, 200) corresponding to h=8 o'clock as illustrated in **Fig. 3**. and **Table 1.** lists all the 12 possible reference points where the top-left corner of the fingerprint image is the point of origin.

The message (msg) was encrypted letter by letter. Each character in the message is converted into its corresponding numerical value (Ψ) using the date-based lookup table which contain (C) characters, **Table 2**. is assumed for the given date with C= 95 corresponding numerical value. The first value of the key will use to cipher the corresponding numerical value of the character as the same of Vigenère cipher.

The reference point (x_o, y_o) will be (33, 200) corresponding to h=8 o'clock as illustrated in **Fig. 3**. and **Table 1.** lists all the 12 possible reference points where the top-left corner of the fingerprint image is the point of origin. The message (msg) was encrypted letter by letter. Each character in the message is converted into its corresponding numerical value (Ψ) using the date-based lookup table which contain (C) characters, **Table 2**. is assumed for the given date with C= 95 corresponding numerical value. The first value of the key will use to cipher the corresponding numerical value of the character as the same of Vigenère cipher. The PM hours will refer to a subtraction operation between the numerical value of the character and the key of encryption, on the other hand, an addition operation for AM hours. The resultant will convert back as character using **Table 2**. Eq. (8) created to illustrate the proposed method clearly.



a.Input Image b. Enhanced Image c. Binary Image



d. Thinned image e. Minutiae position

Figure 2. Image Enhancement and feature extraction Process.

Table 1. Possible reference points.

h (hour)	x_o	y_o	h (hour)	x_o	y_o
1	170	63	7	70	237
2	207	100	8	33	200
3	220	150	9	20	150
4	207	200	10	33	100
5	170	237	11	70	63
6	120	250	12	120	50

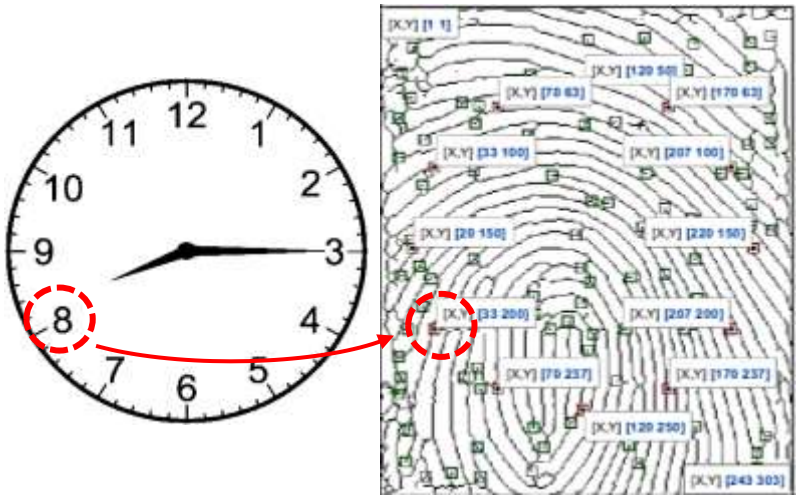


Figure 3. Time-based reference points.

Table 3 shows the distance of minutiae to the reference point (33, 200) which is related to h=8, these distances will be the key. (;^wIGLQn0&&z95) is the ciphertext for the phrase (Ziggurat of Ur) according to Eq. (8).

$$ciphertext(i) = [\Psi_i + (\alpha \times key_i)] mod\ C \quad (8)$$

Where: α is equal to (+1) at AM hours and (-1) at PM hours.
and C is the number of characters in the lookup table and it is assumed to be 95 characters.
The decryption results listed in **Table 4**, show that original message cannot be reconstructed unless the same minutiae combination is used, in other words, the date and time of encryption process. Although the correct date and time is used, attackers will try all possible attempts to discover the correct minutiae combination and spend longtime to find out which reference point that were used as well as the other parameters.

Table 2. Lookup Table for the first of January 2022.

Character	space	!	“	#	$	%	&	‘	(	)	*	=	,	-	.	/	0
Corresponding value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Character	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?	@	A
Corresponding value	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
Character	B	C	D	E	F	G	H	I	G	K	L	M	N	O	P	Q	R
Corresponding value	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
Character	S	T	U	V	W	X	Y	Z	[	~	]	^	_	`	a	b	c
Corresponding value	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67
Character	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
Corresponding value	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84
Character	u	V	w	x	y	z	{	¬	}	|							
Corresponding value	85	86	87	88	89	90	91	92	93	94							

Table 3. Ciphering the phrase (Ziggurat of Ur).

seq	Minutiae for m=15, (K=1.10)		Key [Distance from h=8 (33, 200)]	Message	Ψ	α	[Ψ + (α×key)] mod 95	Cipher text
	x	y						
1	14	42	159	Z	58	+1	27	;
2	16	282	84	i	73	+1	62	^
3	17	200	16	g	71	+1	87	w
4	18	263	65	g	71	+1	41	I
5	19	57	144	u	85	+1	39	G
6	19	145	57	r	82	+1	44	L
7	20	26	174	a	65	+1	49	Q
8	26	111	89	t	84	+1	78	n
9	26	186	16	space	0	+1	16	0
10	27	83	117	o	79	+1	6	&
11	31	169	31	f	70	+1	6	&
12	43	289	90	space	0	+1	90	z
13	56	137	67	U	53	+1	25	9
14	57	73	129	r	82	+1	21	5
15	58	224	35					
⋮	⋮	⋮	⋮					
93	231	139	207					

Table 4. Decryption results for several attempts.

Cipher text Generated in 1-1-2022 8:15 AM	**Message extracted**	**Date and time used for decryption**	**Note**
;^wIGLQn0&&z95	Ziggurat of Ur	1-Jan-2022 8:15 AM	Same time and date
	.9E7I/*JLoPLr?	1- Jan -2022 9:15 AM	One hour different
	g{#9ezw| o*[>q	1- Jan -2022 8:14 AM	One minute different
	wt%}$6O!QOB-uu	14-Sep-2022 8:15 AM	Different date
	wq!#^3:}]NDTq+	14-Sep-2022 12:45 AM	Different date and time
	{S(+x&Ah@<Eu¬W	14-Sep-2022 12:45 PM	Different date and time

6. CONCLUSIONS

It is clear that Vigenère cipher consider very simple to implement and so easy to break by attacker. To beat its weaknesses, this paper proposes a new algorithm to renovate Vigenère substitution cipher by combining it with fingerprint features and time.
The obtained ciphertext was uncorrelated with the plaintext where this algorithm conceals the relationship between them, and the cryptanalysis become more difficult.
On the other hand, the use of fingerprints for their uniqueness as well as the dynamic key length due to its dependence on the number of extracted minutiae will make any brute force attack or Kasiski attack be unsuccessful.
The main points of strength of the proposed method can be summarized by:

- The life time of any generated key is 1 minute.
- There are 720 various key per day yield to 1440 ciphertexts for the same message, 720 ciphertexts for each AM and PM hours.
- Daily change of the corresponding numerical value will fizzle out any attempt based on frequency cryptanalysts.
- The dynamic length of the generated key.

CONFLICT OF INTEREST
The authors confirm that there is no conflict of interest in publishing the present research work.

NOMENCLATURE

$f(x,y)$ = a block of (32×32) pixels in a fingerprint image
$F(u,v)$ = FFT of $f(x,y)$
$g(x,y)$ = enhanced image block in frequency domain
$\acute{f}(x,y)$= enhanced image block
m×n = dimensions of fingerprint image
M×N = dimensions of each fingerprint block
hh:mm PM or AM = the time of key generation
h = hour of generation (from 1 to 12)
m = minute of generation (from 0 to 59)
K = image enhancement factor
L = the key length which is the same of the number of minutiae points
x_n = the position of n^{th} minutiae point on x-axis.
y_n = the position of n^{th} minutiae point on y-axis.
x_o = the position of a reference point on x-axis.
y_o = the position of a reference point on y-axis.
r_o = the radius of the reference cycle.
Ψ = corresponding numerical value for alphabet.
α = equal to (+1) at AM hours and (-1) at PM hours.
C = the number of characters in the encryption domain and it is assumed to be 95 characters.

REFERENCES

Ahmadzadeh, E., Kim, H., Jeong, O., and Moon, I., 2021. A novel dynamic attack on classical ciphers using an attention-based LSTM encoder-decoder model. *IEEE Access*, 9, pp. 60960-60970. doi:10.1109/ACCESS.2021.3074268

Angaye, C.O., Akinyokun, O.C., and Iwasokun, G.B., 2013. Experimental study of minutiae-based algorithm for fingerprint matching. *Computer Science & Information Technology* (CS & IT), pp. 33-47. doi:10.5121/csit.2013.3504

Bhargava, N., Bhargava, R., Mathuria, M., and Dixit, P., 2013. Fingerprint minutiae matching using region of interest. *International Journal of Computer Trends and Technology*, 4(4), pp. 515-518. https://ijcttjournal.org/Volume4/issue-4/IJCTT-V4I4P115.pdf

Dooley, J.F., 2018. *History of cryptography and cryptanalysis: Codes, Ciphers, and their algorithms*. Springer.

Henry E. R., 1900. *Classification and Uses of Fingerprints*. George Routledge and sons.

Ibrahim, D. R., Sen Teh J., and Abdullah R., 2021. An overview of visual cryptography techniques. *Multimedia Tools and Applications*, 80, pp. 31927–31952. doi:10.1007/s11042-021-11229-9

Jegede, A., Udzir, N.I., Abdullah, A. and Mahmod, R., 2017. State of the art in biometric key binding and key generation schemes. IJCNIS 9(3), pp. 333-344. doi:10.17762/ijcnis.v9i3.2388

Jerjees S. A., Esttaifan B. A. and Ismaeel T. Z., 2020. Hybrid Ciphering Method Based on Chaos Logistic Map and Fingerprint Information. *Journal of Engineering Science and Technology*, 15(5), pp. 3013-3024. https://jestec.taylors.edu.my/Vol%2015%20issue%205%20October%202020/15_5_11.pdf

Kako, N. A., Sadeeq, H. T., and Abrahim, A. R., 2020. New symmetric key cipher capable of digraph to single letter conversion utilizing binary system. *Indonesian Journal of Electrical Engineering and Computer Science*, 18 (2), p. 1028. doi:10.11591/ijeecs.v18.i2.pp1028-1034

Kester, Q.A, 2012. A cryptosystem based on Vigenère cipher with varying key. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1 (10), pp. 108–113. https://www.researchgate.net/publication/235618077_A_cryptosystem_based_on_Vigenere_cipher_with_varying_key

Kester, Q.A., 2013. A hybrid cryptosystem based on Vigenère Cipher and columnar transposition Cipher. *International Journal of Advanced Technology & Engineering Research* (IJATER), 3(1), pp. 141–147. doi:10.48550/arXiv.1307.7786

LS-WL, L.A.M. and SUEN, C., 1992. Thinning methodologies comprehensive survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 14(9), pp. 869-885. doi:10.1109/34.161346

Nedjah, N., Wyant, R.S., Mourelle, L.M., and Gupta, B.B., 2019. Efficient fingerprint matching on smart cards for high security and privacy in smart systems. *Information Sciences*, 479, pp. 622-639. doi:10.1016/j.ins.2017.12.038

Omran, S.S., Al-Khalid, A.S., and Al-Saady, D.M., 2011, September. A cryptanalytic attack on Vigenère cipher using genetic algorithm. In 2011 IEEE Conference on Open Systems, pp. 59-64. doi:10.1109/ICOS.2011.6079312

Rahmani, M. K. I., Wadhwa, N., and Malhotra, V., 2012. Alpha-qwerty Cipher: an extended Vigenère Cipher. *Advanced Computing: An International Journal*, 3(3), pp. 107–118. doi:10.5121/acij.2012.3311

Salih, A. M., and Mahmood, S. H., 2019. Digital Color Image Watermarking Using Encoded Frequent Mark. *Journal of Engineering*, 25(3), pp. 81–88. doi:10.31026/j.eng.2019.03.07

Sharif, A., and Sianipar, R., 2018. A combination of Vigenère algorithm and one time pad algorithm in the three-pass protocol. In MATEC Web of Conferences, 197, p. 03008. EDP Sciences. doi:10.1051/matecconf/201819703008

Shiltagh, N. A., Abdullah, M. Z., and Ahmed R. Zarzoor, A. R., 2019, WSN-WCCS: A Wireless Sensor Network Wavelet Curve Ciphering System. *Journal of Engineering*, 25(6), pp. 67–82. doi:10.31026/j.eng.2019.06.06

Subandi, A., Meiyanti, R., Sandy, C. L. M., and Sembiring, R. W., 2017. Three-pass protocol implementation in Vigenère Cipher classic cryptography algorithm with keystream generator modification. Advances in Science, Technology and Engineering Systems Journal, 2(5), pp. 1–5. doi:10.25046/aj020501

Trappe, W., 2006. *Introduction to cryptography with coding theory*. 2nd edition. Pearson Prentice Hall.

Uniyal, D. N., Dobhal, D. G., and Semwal, M. P., 2020. Enhanced security of encrypted text by KDMT: key-domain maximization technique. *International Journal of Recent Technology and Engineering* (IJRTE), 8(5), pp. 1385–1388. doi:10.35940/ijrte.E6326.018520

Willis, A.J., and Myers, L., 2001. A cost-effective fingerprint recognition system for use with low-quality prints and damaged fingertips. *Pattern recognition*, 34(2), pp. 255-270. doi:10.1016/S0031-3203(00)00003-0

Wilson, P., and Garcia, M., 2006. A modified version of the Vigenère algorithm. International Journal of Computer Science and Network Security (IJCSNS), 6(3), pp. 140–143. http://paper.ijcsns.org/07_book/200603/200603C01.pdf

Yang, W., Hu, J., Wang, S., and Stojmenovic, M., 2014. An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures. *Pattern Recognition*, 47(3), pp. 1309-1320. doi:10.1016/j.patcog.2013.10.001

You, X. et al., 2021. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. *Science China Information Sciences*, 64(1), p. 110301. doi:10.1007/s11432-020-2955-6

Zafar, W., Ahmad, T., and Hassan, M., 2014, December. Minutiae based fingerprint matching techniques. In 17th IEEE International Multi Topic Conference 2014, pp. 411-416. IEEE. doi:10.1109/INMIC.2014.7097375