Jewel Journal of Scientific Research (JJSR) 3(1): 79- 87, 2015
©Federal University, Kashere-Nigeria (ISSN: 2384 - 6267)
www.fukashere.edu.ng

A Block Cipher obtained by blending modified playfair Cipher with advanced hill Cipher

Zirra, P. B[*], Wajiga, G. M.[1], Yusuf, S. E.

Department of Mathematics and Computer Science, Federal University, Kashere, Gombe, Nigeria
[1]Computer Science Department, Federal University of Technology, Yola, Nigeria
Author for Correspondence: zirrapeter64@gmail.com

Abstract

In this paper we presented a new technique for secure transmission of message based on modified version of playfair cipher combined with Hill cipher to encrypt and decrypt a message from sender and receiver vice versa. The traditional playfair cipher and Hill cipher methods are based on polyalphabetic cipher of 26 letters which is relatively easy to break because it leaves much of loop holes and a small hundreds of letters, digits and other special characters unused. At each stage of encryption and decryption, two different keys are used to encrypt and decrypt the message according to the modified features of the ciphers. From the cryptanalysis performed in this work, we have found that this cipher thwarts any known plaintext attack, chosen plaintext attack and chosen ciphertext attack.

Keywords: ASCII code, cryptanalysis, inverse of matrix, modular arithmetic, plaintext.

Introduction

In order to provide security to the information that is to be transmitted from sender to receiver on a network or communication systems we have several methods for it. The well known and highly used method for protecting the data during its transmission across the network is encryption. The conventional encryption system consists of plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm which is inefficient considering the major challenges that can be caused by the skilled hackers and intruders. We need a strong encryption algorithm in order to encrypt the plaintext into ciphertext. The sender and receiver must have obtained the secret key in a secure fashion and must keep the key secure (Shrivastava *et al.*, 2013).We proposed a cryptosystem that used Playfair cipher to perform encryption. The resultant is used on Hill cipher to obtain another new encryption. Decrption is obtained in reverse order.

Related work

The Playfair cipher

The Play fair cipher uses a *5* by *5* table containing a key word or phrase.

Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher. To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "Q" to reduce the alphabet to fit, other versions put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constituted the cipher key. To encrypt a message, one would break the message into digraphs (groups of 2 letters). The two letters of the digraph are considered as the opposite corners of a rectangle in the key table (Nisarga *et al*., 2013). Note the relative position of the corners of this rectangle. Then apply the following four rules, in order, to each pair of letters in the plaintext:

i. If both letters are the same (or only one letter is left), add an "*X*" after the first letter. Encrypt the new pair and continue. Some variants of Playfair use "*Q*" instead of "*X*", but any uncommon monograph will do.
ii. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
iii. If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
iv. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important- the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.

To decrypt, use the inverse (opposite) of the last three rules, and the 1st as-is (dropping any extra "*X*"s (or "*Q*"s) that don't make sense in the final message when finished).

Hill cipher

Though Hill cipher is susceptible to cryptanalysis and unusable in practice, still serves an important pedagogical role in both cryptology and linear algebra. It is this role in linear algebra that raises several interesting questions (Kuppuswamy and Chandrasekar, 2011)

Classical Hill cipher was developed by the mathematician Lester Hill in 1970. The encryption algorithm takes in successive plaintext letters P and substitutes for the P ciphertext letters. The substitution is determined by the linear equations in which each character is assigned a numerical value (*A=01, B=02, C=03, …, Z=26*). The general basic equations governing the Hill cipher (Chowdhury *et al*., 2011) are:

$$C = P * K \bmod 26 \qquad (1)$$

and

$$P = K^{-1} * C \bmod 26 \qquad (2)$$

Where P is the plaintext Colum vector, K the encryption key matrix, C the ciphertext, and K^{-1} is the modular arithmetic inverse of K (Sastry and Samson, 2012).

Cofactor of a matrix

If $A = (a_{i,j})$ is a square matrix of order n, then the cofactor of **A** denoted by Cij, is

define by $C_{ij} = (-1)^{i+j} M_{ij}$, where M_{ij} is the minor of the matrix *A*, for1 ≤ i ≤ j ≤ n (Sastry and Samson, 2012)

Determinant of a matrix

If $A = (a_{i,j})$ is a square matrix of order n, then the determinant of **A** is denoted by |**A**| and is defined by Sastry & Samson (2012) as

$$|A| = \sum C_{a_{ij}} . a_{ij} \quad (3)$$

Adjoint of a matrix

Sastry and Samson, (2012) defined the adjoint of a square matrix A denoted by $Adj(A)$ as the transpose of the matrix cofactor of the element $a_{i,j}$ of A.

Therefore,

$$Adj(A) = (c_{i,j})^T \quad (4)$$

Inverse of a matrix

A square matrix A has an inverse if and only if the determinant |A|≠ 0. A matrix possessing an inverse is called non-singular or invertible. The inverse of a square matrix A is a matrix A^{-1} (Zirra and Wajiga, 2011) such that $AA^{-1} = I$, where I is the identity matrix (Santos, 2010).

Given a $2x2$ matrix, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

(5)

It is mathematically defined as

$$A^{-1} = \frac{1}{bc-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} mod\ n,$$

(6)

Where n is any positive integer

Methodology

The proposed crptosystem is based on the combination of modified Playfair cipher in Table 1 and Hill ciphers based on the 95 printable American Code for Information Interchange (*ASCII*) characters with MOD 95 in Table 2 to increase and enhance its resistance towards common attacks. With the proposed scheme, the plaintext message (*M*) with a secrete keyword (K_p) is encrypted using the Playfair cipher rules to produce a ciphertext (*C*) which in turn enciphered with advanced Hill cipher to produce another new ciphertext C_{new}. Figure 1 explains the encryption and decryption processes of the proposed system.

Table 1: Modified Playfair cipher

A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	0	1	2	3
4	5	6	7	8	9	a	b	c	d
E	f	g	h	i	j	k	l	m	n
O	p	q	r	s	t	u	v	w	x
Y	z	+	□	!	‘’	#	$	%	&
‘	(	)	*	`	-	.	/	:	;
<	=	>	?	@	[	\	]	^	_
,	{	|	}	~					

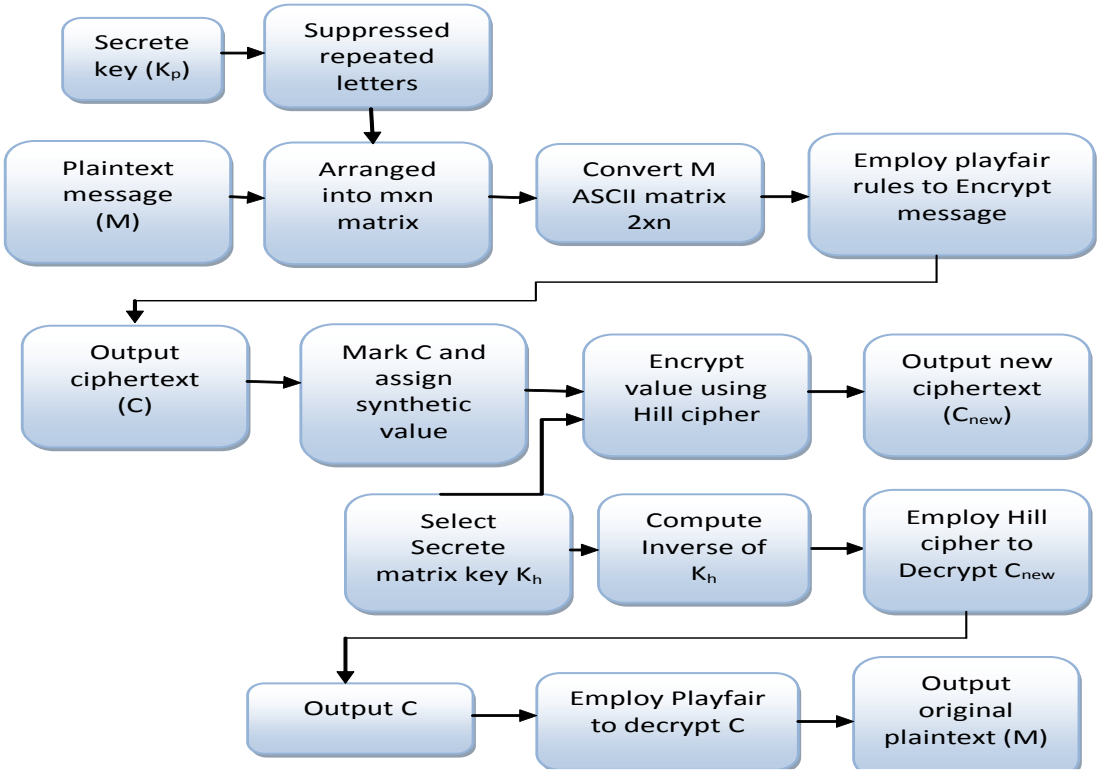

Figure 1: Block diagram explaining the encryption and decryption of the proposed system.

Table 2**:** 95 Printable *ASCII* characters with MOD 95 and their corresponding position numbers

A (1)	B (2)	C (3)	D (4)	E (5)	F (6)	G (7)	H (8)	I (9)	J (10)	K (11)
L (12)	M (13)	N (14)	O (15)	P (16)	Q (17)	R (18)	S (19)	T (20)	U (21)	V (22)
W (23)	X 24()	Y (25)	Z (26)	0 (27)	1 (28)	2 (29)	3 (30)	4 (31)	5 (32)	6 (33)
7 (34)	8 (35)	9 (36)	a (37)	b (38)	c (39)	d (40)	e (41)	f (42)	g (43)	h (44)
i (45)	j (46)	k (47)	l (48)	m (49)	n (50)	o (51)	p (52)	q (53)	r (53)	s (55)
t (56)	u (57)	v (58)	w (59)	x (60)	y (61)	z (62)	! (63)	“ (64)	# (65)	$ (66)
% (67)	& (68)	‘ (69)	((70)	) (71)	* (72)	+ (73)	, (74)	- (75)	. (76)	/ (77)
: (78)	; (79)	< (80)	= (81)	> (82)	? (83)	@ (84)	[(85)	\ (86)	] (87)	^ (88)
_ (89)	` (90)	{ (91)	| (92)	} (93)	~ (94)	□ (95)				

At the time of encryption, □ is used to provide space between two words, @ is used for stuffing between two alphabets if they are repeated in a pair and # will also be used to put at the end to get the last alphabet in pair if the total length comes out to be odd. At the time of decryption □ will be replaced by blank space and the symbol # will be discarded.

The proposed algorithm for encryption and decryption is given below:

Phase-1: Sender site

Step1: Read 95 printable ASCII code (*P*) with its synthetic value as depicted in Table 2.

Step2: Select K_p and form a substitution table by first filling K_p into rows or columns followed by the other *ASCII* characters after suppressed repeated characters.

Step3: Take *M* and convert into a matrix size of *2* by *n*.

Step4: Encrypt *M* using Playfair cipher rules (i-iv) in subsection 2.1 to produce ciphertext (*C)*.

Step5: Assign the corresponding decimal *ASCII* (synthetic) value in Table 2 to the received message *(C*).

Step6: Mark *C* as a linear block.

Step7: Take C and encrypt with secrete invertible key matrix K_h following the Hill cipher as (1) to produce another new ciphertext C_{new}.

Phase-2: Receiver site

Step1: Received message C_{new} is decrypted using K_h^{-1} as in (6) to produce Hill cipher decryption *C*.

Step2: Take *C* and decrypt using the revised steps of the Playfair cipher rules (ii-iv) in subsection 2.1 to display the original message (*M*).

Experimentation of the proposed scheme

Enciphering plaintext

Consider the plaintext (*M*) given below:

The World Bank has given an assistance of $100 billion for the flood disaster victims in the year 2012 in Nigeria. Let us have a fair sharing formula for the affected community.

Let us focus our attention on the first twelve characters of the above plaintext including spaces. This is given by:

The□World□Ba

We select a secrete keyword (K_p):

GSM+2348059570222

Form a substitution Table 3 from Table 1 with K_p, by first filling K_p into rows or columns followed with the remaining ASCII characters after suppressed repeated characters.

Table 3: Substitution table with K_p

G	S	M	+	2	3	4	8	0	5
9	7	A	B	C	D	E	F	H	I
J	K	L	N	O	P	Q	R	T	U
V	W	X	Y	Z	1	6	a	b	c
D	e	f	g	H	i	j	k	l	m
N	o	p	q	R	s	t	u	v	w
X	y	z	□	!	‘’	#	$	%	&
‘	(	)	*	`	-	.	/	:	;
<	=	>	?	@	[	\	]	^	_
,	{	|	}	~					

Next, we partition the plaintext message (M) into a matrix of size 2×6 as follows:

$$M = \begin{pmatrix} T & h \\ e & \square \\ W & o \\ r & l \\ d & \square \\ B & a \end{pmatrix} \quad (7)$$

Apply the Playfair rules in subsection 2.1 to obtain the matrix ciphertext (C)

$$C = \begin{pmatrix} l & O \\ g & y \\ e & y \\ v & h \\ g & x \\ F & Y \end{pmatrix} \quad (8)$$

Thus the ciphertext (C) can be rewritten as:

lOgyeyvhgxFY

The ciphertext (C) from the modified Playfair cipher becomes a new plaintext message (P_h) to Hill cipher encryption algorithm. Replace P_h with their corresponding numerical value in Table 2, to form the linear block ciphertext in Table 4**.**

Table 4: Linear block ciphertext.

Block number	*M*	Blocking C			Synthetic value for *C*		
1		l	O	g	48	15	43
2	The	y	E	y	61	41	61
3	World	v	H	g	58	44	43
4	Ba	x	F	Y	64	6	25

We select $r \times r$ invertible matrix K_h to form the key in (9)

$$K_h = \begin{pmatrix} 1 & 2 & 1 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \quad (9)$$

Using Hill cipher algorithm, encrypt the four blocks of ciphertext in Table 4 based on their corresponding synthetic values to produce the new ciphertext (C_{new}).

The first block consists of the letters **lOg** with equivalent synthetic value of **48**, **15**, and **43** respectively. We then convert the given equivalent synthetic data as a transpose matrix to obtain a new ciphertext of block one (C_{b1}) as in (10)

$$C_{b1} = \begin{pmatrix} 1 & 2 & 1 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 48 \\ 15 \\ 43 \end{pmatrix} mod\ 95 = \begin{pmatrix} 26 \\ 50 \\ 83 \end{pmatrix} \quad (10)$$

Similarly, we take the second, third and fourth blocks to obtain (11)-(13) as in (10)

$$C_{b2} = \begin{pmatrix} 1 & 2 & 1 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 61 \\ 41 \\ 61 \end{pmatrix} mod\ 95 = \begin{pmatrix} 67 \\ 47 \\ 26 \end{pmatrix} \quad (11)$$

$$C_{b3} = \begin{pmatrix} 1 & 2 & 1 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 58 \\ 44 \\ 43 \end{pmatrix} mod\ 95 = \begin{pmatrix} 94 \\ 45 \\ 5 \end{pmatrix} \quad (12)$$

$$C_{b4} = \begin{pmatrix} 1 & 2 & 1 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 60 \\ 6 \\ 25 \end{pmatrix} mod\ 95 = \begin{pmatrix} 2 \\ 40 \\ 28 \end{pmatrix} \quad (13)$$

Therefore, the new encrypted values and C_{new} are given in Table 5

Table 5: New ciphertext (C_{new}) based on Hill cipher

M	Integer value	Playfair cipher text	Hill ciphertext mod 95 value	New encrypted equivalent text (C_{new})
T	20	L	26	Z
H	44	O	50	n
E	41	G	83	?
	95	Y	14	N
W	23	E	28	1
O	51	Y	76	.
R	54	V	94	~
L	48	H	45	i
D	40	G	5	E
	95	X	2	B
B	2	F	40	d
A	37	Y	28	1

Therefore, the final new ciphertext (C_{new}) corresponding to the original plaintext message (M) **The□World□Ba** is thus:

Zn?N1.~iEBd1

Deciphering ciphertext

First we calculate the inverse of the key matrix in (9) to decrypt C_{new} for Hill cipher.

The determinant of the key matrix in (9) is obtained as follows

$$1(5\times 9 - 6\times 8) - 2(4\times 9 - 7\times 6) + 1(4\times 8 - 5\times 7) = 6$$

(14)

We determine its cofactors

$$K_h = \begin{pmatrix} -3 & 6 & -3 \\ -10 & 2 & 6 \\ 7 & -2 & -3 \end{pmatrix} mod\ 95$$

(15)

and its Adjoints

$$Adj(K_h) = \begin{pmatrix} -3 & -10 & 7 \\ 6 & 2 & -2 \\ -3 & 6 & -3 \end{pmatrix} mod\ 95$$

(16)

From the multiplicative inverse module 95 tables, 6^{-1} is 16 mod 95. So the inverse of the key matrix in (9) over our scalar field Z_{95} is calculated as

$$K_h^{-1} = 6^{-1} \begin{pmatrix} -3 & -10 & 7 \\ 6 & 2 & -2 \\ -3 & 6 & -3 \end{pmatrix} mod\ 95 = \begin{pmatrix} -3x16 & 6x16 & -3x16 \\ -10x16 & 2x16 & 6x16 \\ 7x16 & -2x16 & -3x16 \end{pmatrix} mod\ 95$$

$$K_h^{-1} = \begin{pmatrix} -48 & 96 & -48 \\ -160 & 32 & 96 \\ 112 & -32 & -48 \end{pmatrix} mod\ 95 = \begin{pmatrix} 47 & 1 & 47 \\ 30 & 32 & 1 \\ 17 & 63 & 47 \end{pmatrix}$$

(17)

Multiply (17) by each matrix in (10-13) to decrypt the block of ciphertexts $C_{b1}\ to\ C_{b4}$ in (18-21) Thus

$$C_{b1} = \begin{pmatrix} 47 & 30 & 17 \\ 1 & 32 & 63 \\ 47 & 1 & 47 \end{pmatrix} \begin{pmatrix} 26 \\ 50 \\ 83 \end{pmatrix} mod\ 95 = \begin{pmatrix} 48 \\ 15 \\ 43 \end{pmatrix}$$

(18)

The elements (values) of the matrix (18) correspond to the linear blocking ciphertext (C) ***lOg*** in Table 5.

In similar manner we can decrypt the remainder of the block of ciphertexts

$$C_{b2} = \begin{pmatrix} 47 & 30 & 17 \\ 1 & 32 & 63 \\ 47 & 1 & 47 \end{pmatrix} \begin{pmatrix} 67 \\ 47 \\ 26 \end{pmatrix} mod\ 95 = \begin{pmatrix} 61 \\ 41 \\ 61 \end{pmatrix}$$

(19)

The values of matrix (19) correspond to the linear blocking ciphertext (C) ***yey*** in Table 5.

$$C_{b3} = \begin{pmatrix} 47 & 30 & 17 \\ 1 & 32 & 63 \\ 47 & 1 & 47 \end{pmatrix} \begin{pmatrix} 94 \\ 45 \\ 5 \end{pmatrix} mod\ 95 = \begin{pmatrix} 58 \\ 44 \\ 43 \end{pmatrix}$$

(20)

The values of matrix (20) correspond to the linear blocking ciphertext (*C*) ***vhg*** in Table 5.

$$C_{b4} = \begin{pmatrix} 47 & 30 & 17 \\ 1 & 32 & 63 \\ 47 & 1 & 47 \end{pmatrix} \begin{pmatrix} 2 \\ 40 \\ 28 \end{pmatrix} mod\ 95 = \begin{pmatrix} 64 \\ 6 \\ 25 \end{pmatrix}$$

(21)

The values of matrix (21) correspond to the linear blocking ciphertext (*C*) ***xFY*** in Table 5. The corresponding letters of the decrypted values of matrix (18-21) yield the first stage of the decryption using Hill cipher. This become

C = **lOgyeyvhgxFY** (22)

We can recover the original message (***M***) in Table 5 by decrypting the message in (22) in conjunction with Table 3. The receiver partitioned the ciphertext (22) into 2xn matrix and applies Playfair encryption rules (ii-iv) in section 2.1 in reverse as follows:

i. The pair **lO** forms a rectangle, replace it with **Th**
ii. the pair **gy** forms a rectangle, replace it with **e**□
iii. The pair **ey** is in a column , replace it with **Wo**
iv. the pair **vh** forms a rectangle, replace it with **rl**
v. The pair **gx** is in a column , replace it with d□
vi. The pair **FY** is in a column , replace it with **Ba**

Replace the symbol □ with blank space and discard ♦ as discussed in the previous sections, these yield the second stage of the decryption using Playfair cipher. .

Thus the ciphertext **lOgyeyvhgxFY** becomes **The World Ba**

Cryptanalysis and Results

The encryption and decryption techniques were made stronger through the introduction of modified Playfair cipher into modified Hill cipher. In each level of the encryption and decryption there were two different keys used for encipher and another two for decipher.

If we take the first block of C_{new} and K^{-1} and compute its product and then apply a Playfair cipher rules (ii-iv) in subsection 2.1, the result is not equal to **20 44 41** which represented the original plaintext(M). Similarly if we take the second block C_{new} and K^{-1} and compute its product and then apply a Playfair cipher transformation on the result, the output does not transform to **95 23 51** that represented the original plaintext (M) of the and so on.

Therefore, the given cryptosystem is less vulnerable to ciphertext only attack, known plaintext and chosen cipher methods of attacks because of the multiple encryptions and decryptions. This is a clear indication that the proposed scheme is a strong one.

Conclusions

In the proposed scheme the output of modified Playfair classical cipher is infused into a modified Hill cipher to generate multiple ciphertexts. During decryption processes the received ciphertext is transformed from Hill cipher to Playfair cipher. The result indicates that the ciphertext can provide a substantial avalanche protection against ciphertext only attack, known plaintext attack and chosen cipher attack.

References

(2011). Secured message transaction approach by dynamic Hill cipher generation and digest concatenation. *International Journal of Computer Application*, 23(9): 25-31.

Kuppuswamy, P. and Chandrasekar, C. (2011). Enrichment of security through cryptographic public key algorithm based on block cipher. *Indian Journal of Computer Science and Engineering*, 2(2), 347-355

Nisarga, C., Bappadittya, R. and Krishanu, K. (2013). Designing of an encryption technique suitable for wireless ad-hoc sensor network *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(3): 632-637

Santos, D.A. (2010). Linear algebra notes revision. dsantos@ccp.edu

Sastry, V.U.K. & Samson, C. (2012). A modern advanced Hill cipher including a pair of involutory matrices as multiplicands and involving a set of function. *International Journal of Engineering Science and Technology*, 4(7): 3304-3315.

Shrivastava, G. Chouhan, M. & Dhawan, M. (2013). A modified version of extended Plafair cipher (8x8). *International Journal of Engineering and Computer Science* 2(4): 956 - 961

Zirra, P.B. and Wajiga, G.M. (2011). Cryptographic algorithms using matrix inversion as data protection. *International Journal of information and Communication Technology*, 10: 67-83.