Hindawi
Complexity
Volume 2020, Article ID 8316454, 8 pages
https://doi.org/10.1155/2020/8316454

Research Article

Outer-Convex Dominating Set in the Corona of Graphs as Encryption Key Generator

Zehui Shao,[1] **S. Kosari**,[1] **R. Anoos**,[2] **S. M. Sheikholeslami**,[3] **and J. A. Dayap**[4]

[1]*Institute of Computing Science and Technology, Guangzhou University, Guangzhou 510006, China*
[2]*Cebu Technological University, San Fernando Extension Campus, San Fernando, Cebu, Philippines*
[3]*Department of Mathematics, Azarbaijan Shahid Madani University, Tabriz, Iran*
[4]*Department of Mathematics and Sciences, University of San Jose-Recoletos, Cebu, Philippines*

Correspondence should be addressed to S. Kosari; saeedkosari38@yahoo.com

Received 2 April 2020; Accepted 1 August 2020; Published 26 October 2020

Academic Editor: Rosa M. Lopez Gutierrez

In this paper, we present a new type of symmetric encryption by converting the classical monoalphabetic affine cipher into a polyalphabetic cipher. The proposed encryption utilizes the properties of outer-convex dominating set in the corona of graphs to generate random keys from the shared keyword to every character of the message. The new encryption eliminates the weaknesses of affine cipher, thus increasing the level of confidence for exchanging messages.

1. Introduction

The security of a system is highly essential nowadays. In an economic era in which industries are information-intensive, data is considered one of the world's most treasured resources that fuels economic operations; thus, security of information is a significant requirement. With the rapid growth of the information technology power and with the emergence of the innovative technologies, the number of threats a user is supposed to deal with has grown exponentially. For example, information exchange is challenged by issues pertaining to confidentiality, authenticity, and nonrepudiation. The increasing concern of securing data requires a strong algorithm that enables high level of data protection. This necessitates an algorithm of superior quality which is a combination of both performance and security. Cryptography is where security engineering meets mathematics. It provides us with the tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems, yet it is surprisingly hard to do right, particularly when one aims for resistance to different types of adversaries. Cryptography consists of processing plain information (*plaintext*) applying a cipher and producing encoded output (*ciphertext*), meaningless to a third-party who does not know the key. The process of transforming plaintext into ciphertext is called *encryption* and the reverse process is called *decryption*. In cryptography both encryption and decryption phase are determined by one or more keys. The creation of algorithms which enhance protection capabilities continues to be the direction of the growing concern for a secured communication.

One of the simplest methods for encrypting text is the substitution cipher. A substitution cipher replaces one symbol with another. If the symbols in the plain text are alphabetical characters, we replace one character with another. Substitution ciphers can be categorized as either *monoalphabetic ciphers* or *polyalphabetic ciphers*. In monoalphabetic substitution, each character in the plain text is always replaced by the same character in the cipher text regardless of its position in the text. In polyalphabetic substitution, each occurrence of a character may have a different substitute. The relationship between a character in the plain text to a character in the cipher text is one to many [1].

Modern ciphers possess two important properties: diffusion and confusion. The idea of diffusion is to hide the relationship between the cipher text and the plain text. This

will frustrate the adversary who uses the cipher text statistics to find the plain text. The idea of confusion is to hide the relationship between the cipher text and the key. This will frustrate the adversary who tries to use the cipher text to find the key. Diffusion and confusion can be achieved using the concept of a complex cipher known as a product cipher introduced by Shannon [2]. The success and competence of the cryptographic cipher technique depends upon the fact that how difficult it is to be broken or cracked by a cryptanalyst. Affine cipher is a kind of monoalphabetic substitution cipher, in which each letter in the alphabet is converted to its numeric equivalent, encrypted by a simple arithmetical equation, and converted back to the letter. This cipher is defined by the following rule:

(i) Encryption rule: $C \equiv aP + b \pmod{26}$

(ii) Decryption rule: $P \equiv \overline{a}(C - b) \pmod{26}$

Here, C is the ciphertext, P is the plaintext, and $K = (a, b)$ is the shared key such that $0 \leq C \leq 25$ and $0 \leq P \leq 25$ for some $a, b \in Z$ with $\gcd(a, 26) = 1$, and $\overline{a}$ is the multiplicative inverse of a in Z_{26}.

In this encryption scheme, each letter of the original message is replaced by the same cipher substitute. Thus, such cryptographic systems are highly vulnerable to statistical methods of attack since it preserves the frequency, or relative commonness, of individual letters. Affine ciphers can easily make a system noticeably secure by multiplying each plaintext value by a different number and then inserting a shift. Thus, the said affine cipher will become complex and more secured if it will be converted into a polyalphabetic cipher [3].

Domination in graph is seen as a new tool in developing a complex process in encoding messages [4]. Domination is an area in graph theory with numerous research activities. Nowadays, studies in the field of domination have been growing rapidly because of its wide variation of domination parameters and its application such as those found in [5–14]. One of the domination parameters is outer-convex domination number which was introduced by Dayap and Enriquez in [15] and further investigated in [16, 17]. In [15–17], the authors characterized the outer-convex domination in the join of two graphs and outer-convex domination numbers 1 and 2 and characterized the parameter in the corona, composition, and Cartesian product of graphs.

In this paper, we propose a complex process of encoding and decoding messages by converting the monoalphabetic affine cipher into polyalphabetic cipher by using the property of outer-convex dominating set in the corona of two graphs to generate random keys from the shared keyword to every character of the message (see Figure 1).

1.1. Related Works. In [18], they propose a polyalphabetic cipher with diffusion and confusion properties based on the concept of the complex cipher used by combining of Vigenére cipher with Affine cipher. Yamuna et al. [19] presented an encryption mechanism using Hamilton path properties (path that covers all vertices in the graph). They encrypt data twice, first using the Hamilton path and second using the complete graph to impose more secure method. Etaiwi [20] proposed a new symmetric encryption algorithm that uses the concepts of cycle graph, complete graph, and minimum spanning tree to generate a complex cipher text using a shared key. In [5], they provided a method of encrypting any chemical formula using graph domination as a tool for encryption. Here, every chemical formula is converted into a binary string using graph domination and later encrypted using DNA steganography.

1.2. Basic Graph Definitions and Properties. Graph theory is the study of graphs, which are mathematical structures used to formulate models in many problems in business, social sciences, physical sciences, and information systems. In this section, we discuss some of the basic concepts of graph that we will encounter throughout our investigation. The definitions and notations are based on [21].

Definition 1. A graph G consists of a pair $(V(G), E(G))$ where $V(G)$ is a nonempty finite set whose elements are called vertices and $E(G)$ is a set of unordered pairs of distinct elements of $V(G)$. The elements of $E(G)$ are called edges of the graph G. The number of vertices in G is called the order of G. A graph is connected when there is a path between every pair of vertices.

Definition 2. A dominating set for a graph $G = (V(G), E(G))$ is a subset S of $V(G)$ such that every vertex not in S is adjacent to at least one vertex of S.

Definition 3. A subset C of $V(G)$ is convex in a graph G if, for every pair of vertices $x, y \in C$, each $x - y$ geodesic (shortest path, curve, or arc) joining x and y lies completely in C.

Definition 4. Cycle graph is a graph that consists of a single cycle, or in other words, some number of vertices (at least 3) connected in a closed chain.

Definition 5. Path graph is a graph that can be drawn so that all of its vertices and edges lie on a single straight line.

Definition 6. Let G and H be graphs of order m and n, respectively. The corona of two graphs G and H is the graph $G \circ H$ obtained by taking one copy of G and m copies of H, and then joining the i th vertex of G to every vertex of the i th copy of H.

Definition 7. A set S of vertices of a graph G is an outer-convex dominating set if every vertex not in S is adjacent to some vertex in S and $V(G) \backslash S$ is convex. The minimum outer-convex dominating set of G is the minimum cardinality of an outer-convex dominating set of G.

Corollary 1 (see [17]). *Let G be a connected graph of order $m \geq 2$ and H be any graph of order n. The set $S \subset V(G \circ H)$ is a minimum outer-convex dominating set in $G \circ H$ if*

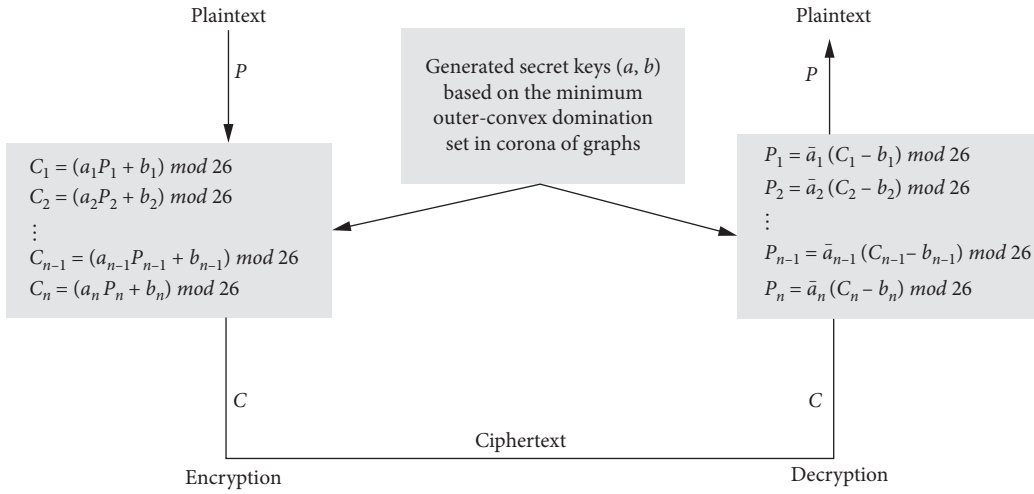

Figure 1: Proposed polyalphabetic affine cipher based on the minimum outer-convex dominating set in the corona of graphs.

$S = \cup_{x \in V(G)} S_x$, *where* $S_x \subseteq V(H^x)$ *is a minimum outer-convex dominating set in* $x + H^x$.

2. Materials and Methods

2.1. Minimum Outer-Convex Dominating Set in $P_n \circ C_4$. In this section, we present on how to determine the minimum outer-convex dominating set in the corona of two graphs using Corollary 1. Here, we let the graph $H = C_4$ (cycle graph of order 4) as a keyword and the graph $G = P_n$ (n is the order of a path graph P_n) as the message to be encrypted.

Example 1. Determine all the minimum outer-convex dominating sets in the graph $G = P_n \circ C_4$.

Solution. the graph illustrated in Figure 2 is the corona of a path graph of order 3 and a cycle graph of order 4.

Using Corollary 1, the elements that consist the minimum outer-convex sets of the graph G are combinations of $\{1,2\}, \{2,1\}, \{2,3\}, \{3,2\}\{3,4\}, \{4,3\}, \{1,4\}$, and $\{4,1\}$. By convention, we let $A = \{1,2\}$, $B = \{2,1\}$, $C = \{2,3\}$, $D = \{3,2\}$, $E = \{3,4\}$, $F = \{4,3\}$, $G = \{1,4\}$, and $H = \{4,1\}$. Thus, the graph G has the minimum outer-convex dominating sets presented in Table 1 (here, we define the minimum outer-convex dominating set as a permutation of the minimum outer-convex dominating set with respect to its position).

The graph in Figure 2 has 512 different sets that satisfies the condition of minimum outer-convex dominating set. In general, the graph $G = P_n \circ C_4$ has 8^n number of different minimum outer-convex dominating sets, where n is the order of graph P_n. To convert the monoalphabetic affine cipher to a polyalphabetic cipher, the key that is used to encrypt and decrypt in every letter of the message must not be the same. Hence, we omit the MOCDS that has the same elements (AAA, BBB, CCC, DDD, EEE, FFF, GGG, and HHH). This implies now that the graph $G = P_n \circ C_4$ has $8^n - n$ number of different minimum outer-convex dominating sets.

2.2. Lists of Tables of Minimum Outer-Convex Dominating Sets (MOCDS) of $G = P_n \circ C_4$ *with Their Corresponding Locator Given the Order of Graph* P_n. In this section, we provide some of the lists of minimum outer-convex dominating sets of $G = P_n \circ C_4$ with their corresponding locator. This locator will be used as part of the proposed encryption scheme.

By convention, we let

$$\begin{matrix} A = (a_1, a_2) & B = (a_2, a_1) & C = (a_2, a_3) & D = (a_3, a_2) \\ E = (a_3, a_4) & F = (a_4, a_3) & G = (a_4, a_1) & H = (a_1, a_4) \end{matrix}, \quad (1)$$

where

(i) a_1, a_2a_3, and a_4 are the equivalent numbers of the first, second, third, and fourth letter of the keyword, respectively.

For $n = 1, 2, 3$, the lists of minimum outer-convex dominating sets of $P_n \circ C_4$ is given in Tables 2–4, respectively.

For the succeeding tables, we follow the pattern presented above (i.e., there is an alternation of letters from right to left with a given pattern of 1, 8, 64, 512, . . .) in listing all the minimum outer-convex dominating sets with their corresponding locator.

2.3. Encryption Algorithm. In this section, we propose a cryptography algorithm to encrypt data to be transmitted using properties of outer-convex dominating set. This algorithm is a symmetric cryptography wherein it uses the concept of shared key that must be predefined and shared between the sender and receiver. The four-letter *keyword* and *key* (c, d) are the keys being shared by the sender and receiver:

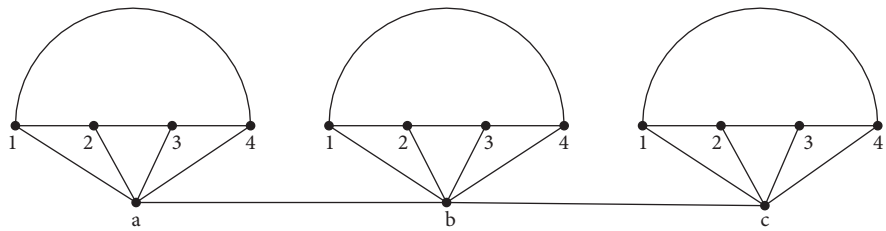

Figure 2: The graph of $G = P_3 \circ C_4$.

Table 1: Minimum outer-convex dominating sets of a graph $G = P_3 \circ C_4$.

AAA	BAA	CAA	DAA	EAA	FAA	GAA	HAA
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
AAH	BAH	CAH	DAH	EAH	FAH	GAH	HAH
ABA	BBA	CBA	DBA	EBA	FBA	GBA	HBA
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
ABH	BBH	CBH	DBH	EBH	FBH	GBH	HBH
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
AGH	BGH	CGH	DGH	EGH	FGH	GGH	HGH
AHA	BHA	CHA	DHA	EHA	FHA	GHA	HHA
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
AHH	BHH	CHH	DHH	EHH	FHH	GHH	HHH

Table 2: Minimum outer-convex dominating sets of G, where $n = 1$.

Locator	MOCDS
0	A
4	E
1	B
5	F
2	C
6	G
3	D
7	H

(1) Draw the graph $G = P_n \circ C_4$, where n is equal to the number of letters of the message to be encrypted.

(2) Write each letter of the original message inside the nodes of P_n and each four-letter keyword inside the nodes of C_4. The equivalent numerical value of each letter of the keyword must be relatively prime with 8^n.

(3) Replace the letters into its equivalent numerical value presented in the encoded Table 5.

(4) Locate and determine the minimum outer-convex dominating set (MOCDS) by using the congruence equation:

$$\text{LMOCDS} \equiv cM + d \pmod{8^n}, \tag{2}$$

as a locator, where

(i) (c, d) is the agreed key such that $c, d \in Z$
(ii) M is the product of the equivalent numerical values of the agreed keyword

Table 3: Minimum outer-convex dominating sets of G, where $n = 2$.

Locator	MOCDS
0	AA
⋮	⋮
7	AH
8	BA
⋮	⋮
15	BH
16	CA
⋮	⋮
23	CH
24	DA
⋮	⋮
31	DH
32	EA
⋮	⋮
39	FA
40	FB
⋮	⋮
47	CA
48	GA
⋮	⋮
55	GH
56	HA
⋮	⋮
63	HH

(iii) n is the number of letters of the original message (note: if the resulting locator will give a minimum outer-convex dominating set of the same element such as AA, BBB, CCCC, and DDDD, reject it and select the next locator in determining the MOCDS).

(5) Encrypt the message using the affine transformation:

$$C \equiv aP + b \pmod{26}, \tag{3}$$

where

(i) (a, b) is the equivalent numerical value in the identified minimum outer-convex dominating set which is adjacent to the letter to be encrypted
(ii) P is the equivalent numerical value of the plaintext
(iii) C is the equivalent numerical value of the ciphertext.

And replace the resulting number into its corresponding letter presented in Table 5.

Table 4: Minimum outer-convex dominating sets of G, where $n = 3$.

Locator	MOCDS
0	AAA
⋮	⋮
7	AAH
⋮	⋮
63	AHH
64	BAA
⋮	⋮
71	BAH
72	BBA
⋮	⋮
79	BBH
⋮	⋮
127	BHH
128	CAA
⋮	⋮
135	CAH
⋮	⋮
191	CHH
192	DAA
⋮	⋮
199	DAH
200	DBA
⋮	⋮
207	DBH
⋮	⋮
255	DHH
256	EAA
⋮	⋮
263	EAH
⋮	⋮
319	EHH
320	FAA
⋮	⋮
327	FAH
328	FBA
⋮	⋮
335	FBH
⋮	⋮
383	FHH
384	GAA
⋮	⋮
391	GAH
⋮	⋮
447	GHH
448	HAA
⋮	⋮
455	HAH
456	HBA
⋮	⋮
463	HBH
⋮	⋮
511	HHH

2.4. Decryption Algorithm. Here, we provide the decryption algorithm that decrypts the message based on the proposed encryption algorithm in the previous section.

(1) Locate and determine the minimum outer-convex dominating set (MOCDS) by using the congruence equation:

$$\text{LMOCDS} \equiv cM + d \pmod{8^n}, \tag{4}$$

as a locator, where

(i) (c, d) is the agreed key such that $c, d \in Z$
(ii) M is the product of the equivalent numerical values of the agreed keyword
(iii) n is the number of letters of the ciphertext (note: if the resulting locator will give a minimum outer-convex dominating set of the same element such as AA, BBB, CCCC, and DDDD, reject it and select the next locator in determining the MOCDS)

(2) Decrypt the message using the affine transformation:

$$P \equiv \overline{a}(C - b) \pmod{26}, \tag{5}$$

where

(i) (a, b) is the equivalent numerical value in the identified minimum outer-convex dominating set which is adjacent to the letter to be encrypted and $\overline{a}$ is the inverse of a in mod 26
(ii) P is the equivalent numerical value of the plaintext
(iii) C is the equivalent numerical value of the ciphertext.

And replace the resulting number into its corresponding letter.

3. Results and Discussion

3.1. Implementation of Modified Affine Cipher

Example 2. Encrypt the message OUR with a keyword FLPR and a key (5, 3).

Solution

(i) Step 1: draw the graph $G = P_n \circ C_4$, where n is equal to the number of letters of the message to be encrypted. Since the message to be encrypted has three letters, we have a graph $G = P_3 \circ C_4$, as shown in Figure 3.

(ii) Step 2: write each letter of the original message inside the nodes of P_n and each four-letter keyword inside the nodes of C_4 (see Figure 4).

See Table 6.

(iii) Step 3: peplace the letters with their equivalent numerical values (see Figure 5).

Table 5: Encoded table based on the letters of the alphabet.

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

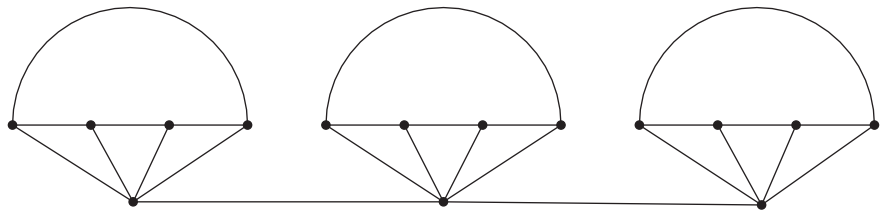

Figure 3: The graph $G = P_3 \circ C_4$.

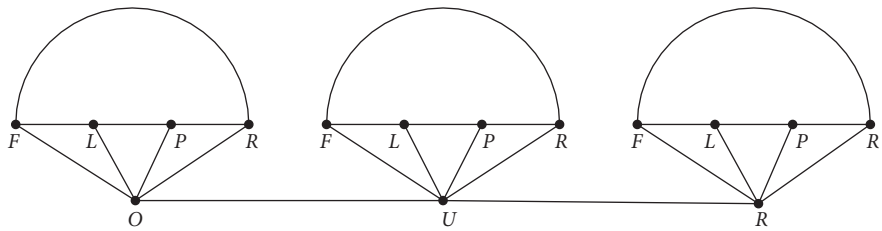

Figure 4: The graph $G = P_3 \circ C_4$ with its corresponding letters.

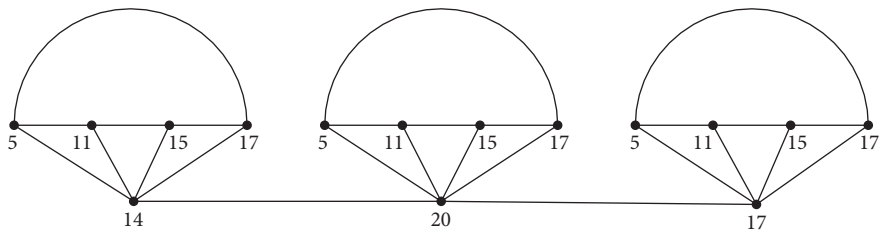

Figure 5: A graph $G = P_3 \circ C_4$ with its equivalent numerical values.

Table 6: Solution on the evaluated affine transformation, $C \equiv (aP + b) \pmod{26}$.

Plaintext	O 14	U 20	R 17
$C \equiv (aP + b) \pmod{26}$	$C \equiv (5(14) + 17) \pmod{26}$ 9	$C \equiv (17(20) + 5) \pmod{26}$ 7	$C \equiv (5(17) + 11) \pmod{26}$ 18
Ciphertext	J	H	S

Table 7: Solution on the evaluated affine transformation, $P \equiv \overline{a}(C - b) \pmod{26}$.

Ciphertext	J 9	H 7	S 18
$P \equiv \overline{a}(C - b) \pmod{26}$	$P \equiv \overline{5}(9 - 17) \pmod{26}$ $P \equiv 21(9 - 17) \pmod{26}$ 14	$P \equiv \overline{17}(7 - 5) \pmod{26}$ $P \equiv 23(7 - 5) \pmod{26}$ 20	$P \equiv \overline{5}(18 - 11) \pmod{26}$ $P \equiv 21(18 - 11) \pmod{26}$ 17
Plaintext	O	U	R

(iv) Step 4: locate and determine the minimum outer-convex dominating set (MOCDS) by using the congruence equation:

$$\text{LMOCDS} \equiv cM + d \pmod{8^n}. \quad (6)$$

The agreed key (c, d) is (5, 3), the M is 14, 025, and n is 3. Thus,

$$\text{LMOCDS} \equiv (5(14,025) + 3) \pmod{8^3} = 496, \quad (7)$$

implying that the desired minimum outer-convex dominating set is on the 496th location. Using the table in Section 2.2, the 496th MOCDS is $\{H, G, A\}$, that is, $\{(5, 17), (17, 5), (5, 11)\}$.

(v) Step 5: encrypt the message using the affine transformation, $C \equiv aP + b \pmod{26}$, and replace the resulting number with its corresponding letter presented on the encoded Table 5.

Example 3. Decrypt the message JHS with a keyword FLPR and a key (5, 3).

Solution. (i) Step 1: locate and determine the minimum outer-convex dominating set (MOCDS) by using the congruence equation

$$\text{LMOCDS} \equiv cM + d \pmod{8^n}. \quad (8)$$

Since $c = 5, d = 3, n = 3$, and $M = 14,025$, it follows that

$$\text{LMOCDS} \equiv (5(14,025) + 3) \pmod{64} = 496. \quad (9)$$

This implies that the desired minimum outer-convex dominating set is on the 496th location. Using the table in Section 2.2, the 496th MOCDS is $\{H, G, A\}$, that is, $\{5, 17, 17, 5, 5, 11\}$.

(ii) Step 2: decrypt the message using the affine transformation:

$$P \equiv \overline{a}(C - b) \pmod{26}, \quad (10)$$

and replace the resulting number with its corresponding letter, see Table 7.

3.2. Security Analysis

(1) The frequency analysis is not possible to perform in this algorithm because the characters are encrypted as one to many. That is, a single character is mapped to many characters while performing encryption.

(2) Kasiski Test fails because the key in this algorithm is not repeating, i.e., the key is based on the locator of the minimum outer-convex dominating set.

4. Conclusions

In this proposed encryption, graph properties are used, specifically, the properties of minimum outer-convex dominating set for encryption. The adversary's knowledge on the affine transformation alone does not guarantee breaking the code. Utilizing the property of outer-convex dominating sets in the corona of two graphs makes it possible for every letter to have its corresponding key. It is shown that the total number of combinations of minimum outer-convex dominating sets is 8^n, where n is the size of the message. These features of the proposed method of encryption increase the difficulty of unauthorized parties to gain access to the intelligible message. The proposed algorithm overcomes the existing drawbacks of the classical affine encryption scheme, thus promoting a more secure information and communication. This study paved a way to new research on applying and evaluating different domination parameters as tool for a more secured encryption algorithm.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Key R&D Program of China (Grant no. 2019YFA0706402) and Natural Science Foundation of Guangdong Province under Grant 2018A0303130115.

References

[1] C. Paar and J. Pelzl, "Introduction to public-key cryptography," in *Understanding Cryptography*, pp. 149–171, Springer, Berlin, Germany, 2010.

[2] C. E. Shannon, "Communication theory of secrecy systems∗," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[3] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, CRC Press, Boca Raton, FL, USA, 2014.

[4] M. Yamuna and A. Elakkiya, "Unique γ-set in text encryption," *Journal of Engineering and Interdisciplinary Research*, vol. 2, pp. 16–21, 2015.

[5] M. Yamuna and K. Karthika, "Chemical formula: encryption using graph domination and molecular biology," *International Journal of ChemTech Research*, vol. 5, no. 6, pp. 2747–2756, 2013.

[6] D. Z. Du and P. J. Wan, *Connected Dominating Set: Theory and Applications*, Springer, New York, NY, USA, 2012.

[7] A. H. Karbasi and R. E. Atani, "Application of dominating sets in wireless sensor networks," *International Journal of Security and its Applications*, vol. 7, no. 4, pp. 185–202, 2013.
[8] J. A. Dayap and E. Enriquez, "Disjoint secure domination in the join of graphs," *Recoletos Multidisciplinary Research Journal*, vol. 4, no. 2, pp. 11–22, 2016.
[9] C. M. Loquias, E. L. Enriquez, and J. A. Dayap, "Inverse clique domination in graphs," *Recoletos Multidisciplinary Research Journal*, vol. 4, no. 2, pp. 23–34, 2016.
[10] M. Dettlaff, S. Kosari, M. Lemańska, and S. M. Sheikholeslami, "The convex domination subdivision number of a graph," *Communications in Combinatorics and Optimization*, vol. 1, pp. 43–56, 2016.
[11] E. Enriquez, V. Fernandez, T. Punzalan, and J. A. Dayap, "Perfect outer-connected domination in the join and corona of graphs," *Recoletos Multidisciplinary Research Journal*, vol. 4, pp. 1–8, 2017.
[12] J. A. Dayap, J. P. Dequillo, W. V. Rios, R. M. T. Telen, and A. Q. Sollano, "Securing chemical formula using poly-alphabetic Affine cipher," *Journal of Global Research in Mathematical Archives*, vol. 6, pp. 6–14, 2019.
[13] J. A. Dayap, J. S. Dionsay, and R. T. Telen, "Perfect outer-convex domination in graphs," *International Journal of Latest Engineering Research and Applications*, vol. 3, no. 7, pp. 25–29, 2018.
[14] J. A. Dayap, R. Alcantara, and R. Anoos, "Outer-weakly convex domination number of graphs," *Communications in Combinatorics and Optimization*, vol. 5, no. 2, pp. 207–215, 2020.
[15] J. A. Dayap and E. L. Enriquez, "Outer-convex domination in graphs," *Discrete Mathematics, Algorithms and Applications*, vol. 12, no. 1, p. 2050008, 2020.
[16] J. A. Dayap and E. L. Enriquez, "Outer-convex domination in the composition and Cartesian product of graphs," *Journal of Global Research in Mathematical Archives*, vol. 6, pp. 34–41, 2019.
[17] J. A. Dayap, "Outer-convex domination in the corona of graphs," *TWMS Journal of Applied and Engineering Mathematics*, In press.
[18] T. M. Aung, H. H. Naing, and N. N. Hla, "A complex transformation of monoalphabetic cipher to polyalphabetic cipher: (Vigenère-Affine cipher)," *International Journal of Machine Learning and Computing*, vol. 9, no. 3, pp. 296–303, 2019.
[19] M. Yamuna, M. Gogia, A. Sikka, and M. Jazib Hayat Khan, "Encryption using graph theory and linear algebra," *International Journal of Computer Applications*, vol. 5, no. 2, pp. 102–107, 2012.
[20] W. Etaiwi, "Encryption algorithm using graph theory," *Journal of Scientific Research and Reports*, vol. 3, no. 19, pp. 2519–2527, 2014.
[21] G. Chartrand and P. Zhang, *A First Course in Graph Theory*, Courier Corporation, Chelmsford, UK, 2012.