International Transactions on Electrical Engineering and Computer Science
S. A. Alabady et.al., Vol: 5, No: 1, pp: 44-52, March 2026

Enhancing Image Security in IoT Environments Using a Modified Vigenère Cipher Algorithm

Salah Abdulghani Alabady[1], Thabita Fawaz Shawkat[1], Amina Waad Adrees[1], Dani Zuhair Elias[1]

Abstract: The Internet of Things (IoT) represents a technologically optimistic future where objects will be connected to the internet and make intelligent collaborations with other objects anywhere, anytime. The described technical architecture of the IoT has an impact on the security and privacy of the involved stakeholders. Privacy includes the concealment of personal information as well as the ability to control what happens with this information. By security we mean the degree of resistance to, or protection of the IoT infrastructure and applications. Many of these devices are easy targets for intrusion. The IoT enables the exchange of multimedia data in a wide variety of applications. Therefor Ensuring confidentiality and privacy is critical when it comes to sharing images over unsecured networks. The security of multimedia data in digital distribution networks is commonly provided by encryption, which is the mathematical process that transforms a plaintext message into unintelligible ciphertext (confused). Vigenère cipher algorithm method is used for securing data in the form of digital images; this paper proposes a method to encrypt an image based on one of the primitive text encryption algorithms Vigenère Cipher. The results show that the original Vigenère algorithm is not good and not suitable for image encryption. On the other hand the proposed algorithm shows there are improvements in the process of encoding images (black / white and color images) using a symmetric key, same key is used for both encryption and decryption.

Keywords: Internet of Things (IoT), Image Encryption, Vigenère Cipher, Multimedia Security, Symmetric Key Cryptography, Privacy Protection

1. Introduction

The Internet of Things (IoT) enables various devices that we use daily to interact with each other via the Internet. This ensures the devices are smart and send the information to a centralized system, which will then monitor and take actions according to the task given to it [1].

History
Received: 25-02-2025; Revised: 15-08-2025;
Accepted: 10-09-2025

S. A. Alabady
eng.salah@uomosul.edu.iq

[1]Computer Engineering Department, College of Engineering, University of Mosul – 41002, Iraq

Hiding the content of data that are sent over an insecure channel has become one of the most important processes of some applications [2]. Data in the form of text, images, videos and audio is multiplying exponentially. So, there is a need to store, maintain and secure this incessant data efficiently to ensure data integrity. Digital images are one of the commonly used data [3]. The images make up a sizable portion of multimedia. National-security agencies, military, and diplomatic issues, for instance, all rely heavily on images for communication. Because such images might contain extremely confidential information, users must entail extreme protection when storing them in an untrustworthy repository. The fundamental goal of protecting images is to ensure their integrity, confidentiality and authenticity in order to secure images, cryptography can be

https://doi.org/10.62760/iteecs.5.1.2026.141

applied [4-5]. Cryptographic algorithms generally fall into two categories, which are symmetric key algorithms and asymmetric key algorithms. Symmetric key algorithms use the same key between the sender and the recipient. As for asymmetric algorithms use a public key and a secret key to encrypt and decrypt the data [6]. Encryption is one of the approaches that may be used to make images more secure. Encryption can be defined as one of the processes which use a key for transforming images into cryptic images. In addition, by using an approach of decryption on cipher image that is typically a reverse execution regarding encryption, users might get the original image. So far, many image encryption techniques are proposed based on the properties of the pixels in the image. Vigenère cipher, a poly-alphabetic cipher, uses a symmetric cipher key for encrypting and decrypting the text. It is very easy to understand and implement. It remained unbreakable for centuries and is more resistant to letter frequency analysis than the simple alphabetic substitution [3]. However, advancements in cryptanalysis have exposed the Vigenère cipher's weaknesses, particularly its susceptibility to the Kasiski examination and frequency analysis when the keyword length is known or guessed. These vulnerabilities limit its effectiveness in modern cryptographic applications. A table known as Vigenere table or Vigenere square is used in Vigenere cipher to make substitution in accordance with the key. Basically, the table is a 26×26 matrix, which means that the English alphabets are written 26 times in different rows, reflecting diverse possible shifts. Obviously, both the table and substitution are used and arranged according to the various shift values that are derived from the key. These clusters behave similarly to image segmentation that divided homogenously [3], [7]. This paper proposes an innovative encryption method aimed at facilitating secure and safe data communication. The Vigenère cipher has been augmented and modified to incorporate extended ASCII code in lieu of solely relying on ASCII code, in addition to the inclusion of alphabets, numerals, and symbols. Furthermore, a swapping operation has been executed. These enhancements are intended to elevate the algorithm's complexity and attain a heightened level of encryption. Additionally, this modification serves to strengthen the security of the Vigenère cipher. The results show that the original Vigenère algorithm is not good and not suitable for image encryption. On the other hand, the proposed algorithm shows there are an improvement in the process of encoding images.

This research is structured into five main sections. Section 1 introduces the study, outlining its importance, goals, and overall scope. Section 2 provides a thorough review of existing literature, summarizing relevant previous work and identifying the research gaps this study aims to fill. Section 3 describes the methodology, including the design and implementation of the proposed algorithm used to meet the research objectives. Section 4 presents and analyzes the results, interpreting their significance in relation to the study's aims. Section 5 concludes the research by highlighting the main findings and offering recommendations for future work.

2. Related Work

This section presents an overview of previous research efforts aimed at enhancing the Vigenère cipher encryption algorithm. Gerhana et al. [8] focused on applying the Vigenère cipher to digital image encryption. Their study demonstrated the algorithm's effectiveness in securing image data of varying capacities, suggesting its suitability for safeguarding digital images in practical security applications. Kester et al. [9] introduced a hybrid encryption approach combining the columnar transposition cipher and the Vigenère cipher. In this method, plaintext is first encrypted using the transposition cipher and then processed with the Vigenère cipher, followed by cryptanalysis for decryption, thus enhancing overall security.

Senthil et al. [10] applied rigorous mathematical concepts such as key generators and their fundamental roots to propose novel variations of the Vigenère and Caesar ciphers. These modifications followed a systematic scientific approach to improve the consistency and robustness of both encryption methods. Purnama and Rohayani [11] proposed a key substitution encryption framework targeting the limitations of traditional confusion-diffusion structures. Their architecture aimed to enhance both security and computational performance by applying an adaptable key scheme for encrypting different image types. Saraswat et al. [12] extended the classical

Vigenère table by incorporating numbers, thereby allowing the encryption of digital data and increasing resistance to cryptanalysis. The inclusion of numerical values reduced text size and complicated the decryption process for attackers.

Uniyal et al. [13] introduced an adaptation of the Caesar cipher by modifying the consonant alphabet and dividing it into segments to accommodate new vocalizations. This structural change aimed to improve the cipher's versatility and decipherability. Rahmani et al. [14] expanded the character set of the traditional Vigenère cipher from 26 to 92 characters. This adjustment allowed for more diverse communication, such as password encryption, making messages and keys harder to decipher due to the inclusion of symbols and special characters. Soofi et al. [15] tackled the weaknesses of the Vigenère cipher against Kasiski and Friedman attacks. Their proposed method utilized eight unique tables in which each alphanumeric character was mapped to a distinct numerical value, including customized values for spaces, thus enhancing the robustness of the cipher.

Omolara et al. [16] developed a hybrid Caesar-Vigenère cipher characterized by a high level of diffusion and confusion. By integrating alphabets, numbers, and symbols into the encryption process, the resulting cipher became more complex and resistant to classical decryption techniques. Song et al. [17] proposed modifications to the Vigenère key stream generator for use in a three-pass protocol. The system was tailored to encrypt 26-character English alphabet messages while addressing issues of key stream predictability and enhancing protection levels. Subandi et al. [18] suggested combining the Vigenère cipher with modern stream cipher techniques to improve reliability. This hybrid approach resulted in stronger security properties compared to using the Vigenère cipher alone, proving especially beneficial for applications requiring high levels of protection. Kartha and Paul [19] introduced a method based on key domain maximization within a finite field. Their technique utilized a randomly generated main key to derive both encryption and decryption keys, enhancing the algorithm's unpredictability and resistance to attacks.

3. Materials and Methods

3.1 Design and implementation of improved Vigenère algorithm

The Vigenère cipher is a method of encrypting alphabetic text that uses multiple Caesar ciphers based on the letters of a keyword, forming a simple form of polyalphabetic substitution [20]. By applying several Caesar ciphers, the Vigenère method disrupts the frequency patterns typically present in a basic Caesar cipher. This technique is named after Blaise de Vigenère, who introduced it in the 16th century at the French court of King Henry III. For many years, the Vigenère cipher was regarded as secure. However, in 1917, it was broken by cryptanalysts Friedman and Kasiski, who identified repeated segments in the ciphertext and used them to determine the length of the encryption key. Once the key length was known, the ciphertext could be divided into columns, each corresponding to a Caesar cipher that could then be individually deciphered. Over time, various modifications have been proposed to enhance the security of the Vigenère cipher [21]. From an algebraic perspective, the Vigenère cipher can also be expressed mathematically. Assuming the letters A to Z represent the numbers 0 through 25, encryption using a key K.

K is performed by adding corresponding values modulo 26 [9], [22], as (1).

$$C_i = \mathrm{E}(P_i + K_i)\mathrm{mod}26 \quad (1)$$

And decryption D using the key K, indicated in (2),

$$P_i = \mathrm{D}(C_i - K_i)\mathrm{mod}26 \quad (2)$$

In this case, C refers to the ciphertext, P for the plaintext character, and K to the key. The decryption function is represented by D. A table, like the one in Fig. 1, could also be used in the Vigenère cipher process. We can express the Vigenère cipher in the following fashion. Assuming a plaintext letter sequence and a letter sequence key, the ciphertext letter sequence can be computed as follows in (3),

$$C = C_0, C_1, C_2 \ldots \ldots C_{n-1} = E(k,p) = E(K_0, K_1, K_2 \ldots \ldots K_{m-1}), (P_0, P_1, P_2 \ldots \ldots P_{M-1}) = (P_0 + K_0)mod26, (P_1 + K_1)mod26 \ldots . (P_{m-1} + K_{m-1})mod26, (P_m + K_0)mod26 \quad , \quad (P_{m+1} + K_1)mod26, (P_{m-1} + K_{m-1})mod26, (P_m + K_0)mod26, (P_{m+1} + K_1)mod26 \quad (3)$$

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Fig. 1: Vigenere square

Table. 1: The expressed numerically based on the category

Category	Expressed numerically													
Key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
Plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
Ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19
Key	19	8	21	4	3	4	2	4	15	19	8	21	4	19
Plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5	3
Ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9	22

Therefore, the first letter of the key is added to the plaintext's first letter, mod 26, followed by the addition of the second letter, and so on, up to the plaintext's first letter. The key letters are repeated for the remaining letters in the plaintext. Until the entire plaintext sequence is encrypted, this process is repeated [22]. A key that is the same length as the message is required to encrypt it. The key is typically a recurring keyword. For example, if the keyword is deceptive, the message "we are discovered, save yourself" is encrypted as follows.

key: deceptivedeceptivedeceptive;
plaintext: wearediscoveredsaveyourself;
ciphertext:
ZICVTWQNGRZGVTWAVZHCQYGLMGJ.

Expressed numerically, we have the result (Table 1). The fact that this encryption has numerous ciphertext letters (one for each distinct letter of the keyword) for every plaintext letter gives it strength. As a result, the letter frequency data is hidden. But not all of the plaintext structure's knowledge is gone [23]. The Vigenère cipher's primary flaw, however, was found to be its repeating key, which leaves it open to frequency analysis via kasiski attack and computation of the coincidence index [24]. The encryption/ decryption Vigenère cipher is shown in Fig. 2.

3.2 The stages of design and implementation for the improved Vigenère algorithm

This section explains the steps that are proposed for improving the Vigenère algorithm.

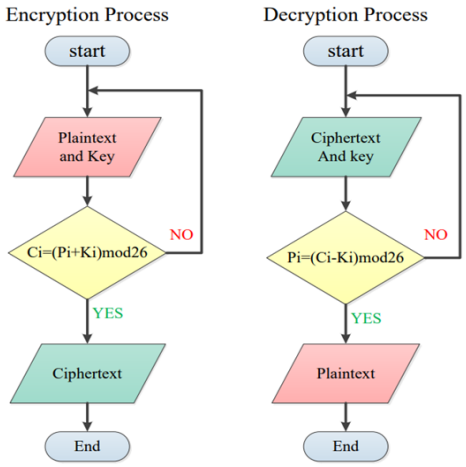

Fig. 2: Vigenere encryption and decryption process

Fig. 3 shows the flowchart of steps that are proposed to improve the Vigenère algorithm. The detailed steps of design and implementation for the Improved Vigenère Algorithm are:

- Read the current input text (each time read 4 byte or 4 characters)
- Perform a swap operation
- Swap character 1 with character 3
- Swap character 2 with character 4
- Perform the original Vigenère algorithm
- Repeat steps on all blocks until the entire input text is finished.

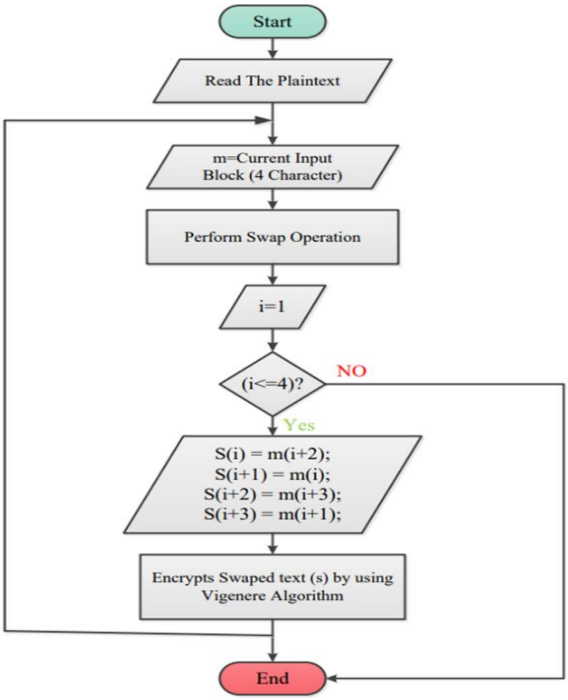

Fig. 3: Flowchart of encryption steps for the improved Vigenere algorithm

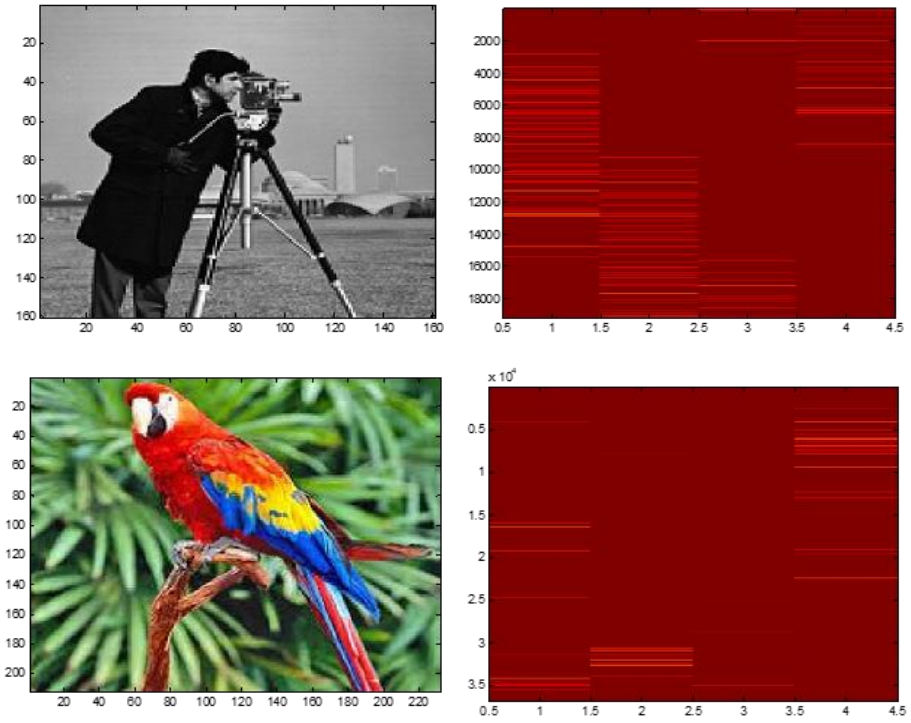

Fig. 4: Results of improved Vigenere algorithm, using key = 1234

4. Results and Discussion

The findings of this study reveal important insights into the performance and security benefits of applying the improved Vigenère cipher to image encryption using a pixel swapping technique. The primary goal of this enhancement was to increase the complexity of the original cipher while preserving its lightweight nature and computational efficiency.

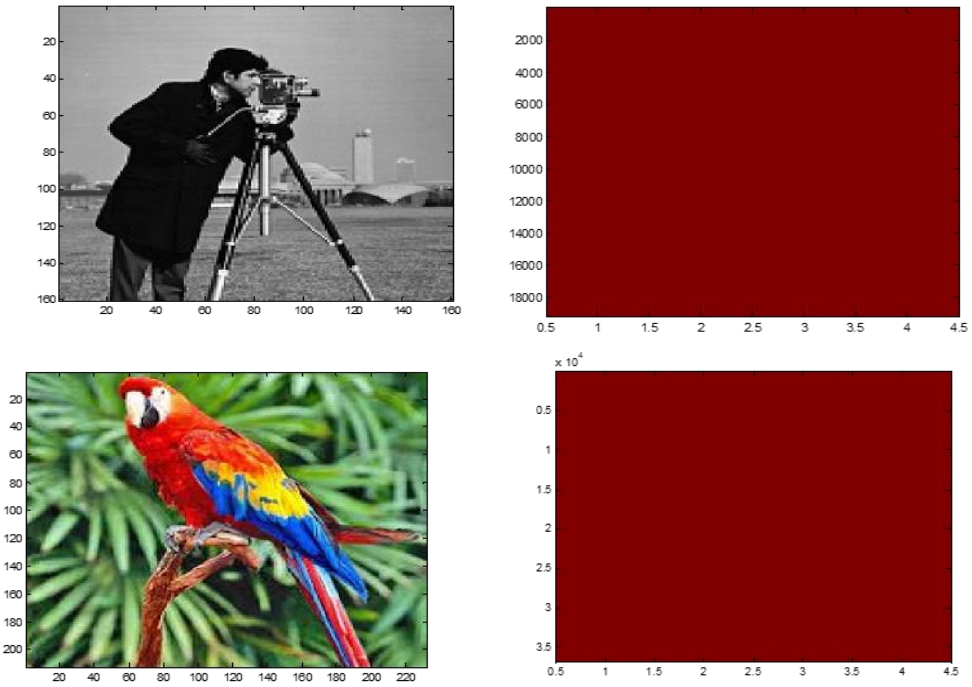

Fig. 5: Results of improved Vigenere algorithm, using key = ABCD

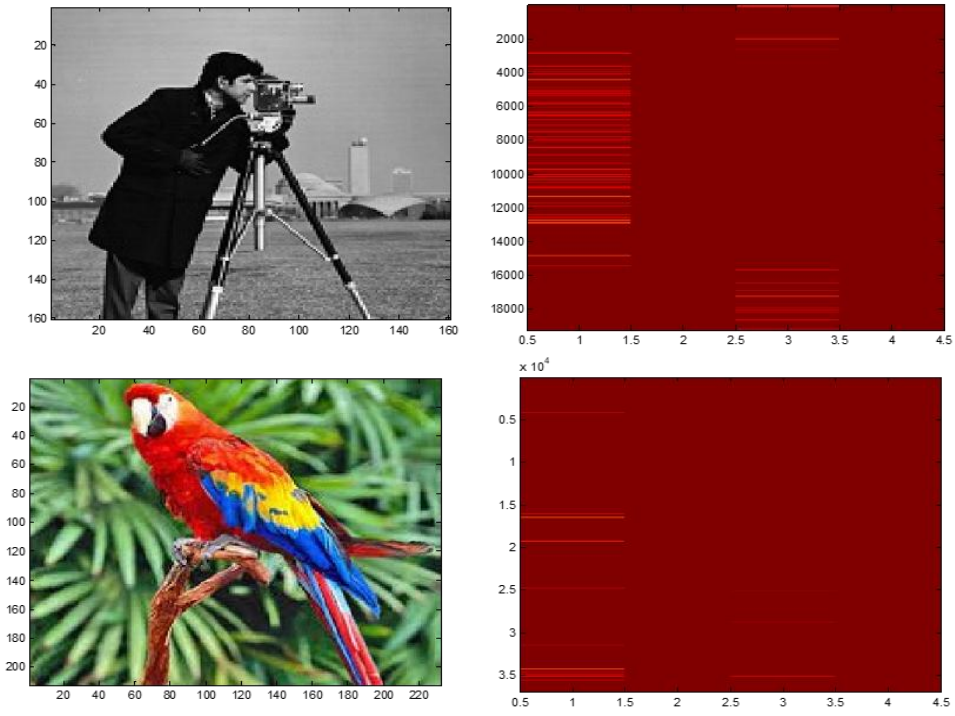

Fig. 6: Results of improved Vigenère algorithm, using key = 1A3B

In this approach, the image is read in blocks of four pixels, and a swap operation is applied where the first pixel is exchanged with the third, and the second with the fourth, before the encryption process begins. This preprocessing step disrupts the original spatial correlation of the image data, adding a layer of confusion that strengthens the encryption. After the swap, the traditional Vigenère cipher is applied to the modified pixel values using a predefined key as indicated in Fig. 4, Fig. 5 and Fig. 6. The results demonstrated a noticeable increase in resistance to common cryptanalytic techniques such as frequency analysis and pattern detection, which are typically more effective against structured data like images. Furthermore, the encryption and decryption processes introduced minimal performance overhead, making the method suitable for resource-limited environments. Although this technique enhances security through added complexity, it also retains the original algorithm's simplicity, making it both practical and efficient for real-time image encryption applications. Future improvements could focus on integrating secure key management systems to further strengthen the overall encryption framework.

5. Conclusion

This paper presents a modified version of the Vigenère cipher algorithm for image encryption by utilizing pixel swapping techniques. Instead of operating on traditional character data, the algorithm works directly with the image's pixel values. Before applying the Vigenère encryption, each block of four pixels undergoes a swap operation where the first pixel is exchanged with the third, and the second is exchanged with the fourth. This pre-processing step increases the randomness in the image data and introduces a high level of diffusion and confusion, making the encrypted image more secure and resistant to analysis. The encryption process was implemented using MATLAB and tested on various images to evaluate performance and security. The results show that the modified algorithm significantly enhances the complexity of the encryption, making it more difficult for attackers to retrieve the original image through brute-force or statistical analysis. The use of pixel-based transformations, combined with the Vigenère cipher, results in a strong and efficient encryption approach suitable for securing image data.

Acknowledgment

The author expresses sincere gratitude to Prof. Dr. Salah Abdulghani Alabady, for continuous guidance and encouragement. Appreciation is also extended to the administration of the computer engineering department for their support.

Funding

The authors did not receive support from any organization for the submitted work.

Data Availability Statement

Data sharing does not apply to this article as no datasets were generated or analyzed during the current study.

Conflict of Interest

The authors declared “No conflict of interest”.

CRediT authorship contribution statement

Conceptualization, SAA, TFS and AWA; methodology, SAA; software, TFS; validation, DZE, TFS and AWA; formal analysis, SAA; investigation, TFS; resources, AWA; data curation, TFS; writing—original draft preparation, AWA; writing—review and editing, AWA and DZE; visualization, SAA; supervision, SAA; project administration, SAA; funding acquisition, SAA. All authors have read and agreed to the published version of the manuscript. Authorship must be limited to those who have contributed substantially to the work reported.

References

[1] S. A. Kumar, T. Vealey and H. Srivastava, “Security in Internet of Things: Challenges, Solutions and Future Directions”, *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA, pp. 5772 - 5781, 2016. https://doi.org/10.1109/HICSS.2016.714

[2] N. A. Al-Romema, A. S. Mashat, and I. Albidewi, "New chaos-based image encryption scheme for RGB components of color image”,

Computer Science and Engineering, Vol. 2, No. 5, pp. 77-85, 2012. [Cross Ref]

[3] V. V. K. Reddy and S. Bhukya, "Encrypt and decrypt image using vigenere cipher", *International Journal of Pure and Applied Mathematics*, Vol. 118, No. 24, pp. 1 - 8, 2018. [Cross Ref]

[4] E. A. Jameel and S. A. Fadhel, "Digital Image Encryption Techniques: Article Review", *Technium*, Vol. 4, No. 2, pp. 24 - 35, 2022. https://doi.org/10.47577/technium.v4i2.6026

[5] A. Susanto, T. H. Khotimah, M. T. Sumadi, J. Warsito, and R. Rihartanto, "Image encryption using vigenere cipher with bit circular shift", *International Journal of Engineering and Technology*, Vol. 7, No. 2, pp. 62 - 64, 2018. [Cross Ref]

[6] R. Darari, E. Winarko, and A. Damayanti, "Encryption and decryption application on images with hybrid algorithm Vigenere and RSA", *Contemporary Mathematics and Applications*, Vol. 2, No. 2, pp. 109 - 117, 2020. https://doi.org/10.20473/conmatha.v2i2.23855

[7] O. F. Mohammad, M. Shafry, M. S. M. Rahim, S. Rafeeq, R. M. Zeebaree, and F. Y. H. Ahmed, "A survey and analysis of the image encryption methods", *International Journal of Applied Engineering Research*, Vol. 12, No. 23, pp. 13265-13280, 2017. [Cross Ref]

[8] Y. A. Gerhana, E. Insanudin, U. Syarifudin and M. R. Zulmi, "Design of digital image application using vigenere cipher algorithm", *2016 4th International Conference on Cyber and IT Service Management*, Bandung, Indonesia, pp. 1 - 5, 2016. https://doi.org/10.1109/CITSM.2016.7577571

[9] Q. A. Kester "A cryptosystem based on Vigenère cipher with varying key", *International Journal of Advanced Research in Computer Engineering & Technology*, Vol. 1, No. 10, pp. 108 - 113, 2012. [Cross Ref]

[10] K. Senthil, K. Prasanthi and R. Rajaram, "A modern avatar of Julius Ceasar and Vigenere cipher", *2013 IEEE International Conference on Computational Intelligence and Computing Research*, Enathi, India, pp. 1-3, 2013. https://doi.org/10.1109/ICCIC.2013.6724170

[11] B. Purnama and A. H. H. Rohayani "A new modified caesar cipher cryptography method with legibleciphertext from a message to be encrypted", *Procedia Computer Science*, Vol. 59, pp. 195 - 204, 2015. https://doi.org/10.1016/j.procs.2015.07.552

[12] A. Saraswat, C. Khatri, Sudhakar, P. Thakral, and P. Biswas, "An extended hybridization of vigenére and caesar cipher techniques for secure communication", *Procedia Computer Science*, Vol. 92, pp. 355 - 360, 2016. https://doi.org/10.1016/j.procs.2016.07.390

[13] N. Uniyal, G. Dobhal, and P. Semwal, "Enhanced security of encrypted text by KDMT: Key-domain maximization technique", *International Journal of Recent Technology and Engineering*, Vol. 8, No. 5, pp. 1385 - 1388, 2020. http://www.doi.org/10.35940/ijrte.E6326.018520

[14] K. I. Rahmani, N. Wadhwa, and V. Malhotra, "Alpha Qwerty Cipher: An Extended Vigenere Cipher", *Advanced Computing*, Vol. 3, No. 3, pp. 107 - 118, 2012. https://doi.org/10.5121/acij.2012.3311

[15] A. A. Soofi, I. Riaz, and U. Rasheed, "An enhanced vigenere cipher for data security", *International Journal of Scientific & Technology Research*, Vol. 5, No. 3, pp. 141 - 145, 2016. [Cross Ref]

[16] O. E. Omolara, A. I. Oludare, and S. E. Abdulahi, "Developing a modified Hybrid Caesar cipher and Vigenere cipher for secure Data Communication", *Computer Engineering and Intelligent Systems*, Vol. 5, No. 5, pp. 34 - 46, 2014. [Cross Ref]

[17] Y. Song, Z. Zhu, W. Zhang, H. Yu and Y. Zhao, "Efficient and Secure Image Encryption Algorithm Using a Novel Key-Substitution Architecture", *IEEE Access*, Vol. 7, pp. 84386 - 84400, 2019. https://doi.org/10.1109/ACCESS.2019.2923018

[18] A. Subandi, M. S. Ladia, R. W. Sembiring, M. Zarlis and S. Efendi "Vigenere cipher algorithm modification by adopting RC6 key expansion and double encryption process", *IOP Conference Series: Materials Science and Engineering*, Vol. 420, art. no. 012119, 2018. https://doi.org/10.1088/1757-899X/420/1/012119

[19] R. S. Kartha and V. Paul, "Survey: recent modifications in Vigen*ere Cipher", IOSR Journal of Computer Engineering*, Vol. 16, No. 2, pp. 49 - 53, 2014. [Cross Ref]

[20] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data security using vigenère cipher and goldbach codes algorithm", *International Journal of Engineering Research & Technology*, Vol. 6, No. 1, pp. 360 - 363, 2017. [Cross Ref]

[21] A. A. M. Aliyu and A. Olaniyan "Vigenere cipher: trends, review and possible modifications", *International Journal of Computer Applications*, Vol. 135, No. 11, pp. 46 - 50, 2016. https://doi.org/10.5120/ijca2016908549

[22] D. Gyasi-Nyarko, E. Freeman, M. M. Ujakpa, W. Amponsah and S. O. Amoako, "A Systematic Review of Public Key Cryptography: Implementation, Challenges and Future Opportunities", *2025 IST-Africa Conference (IST-Africa)*, Nairobi, Kenya, pp. 1 - 15, 2025. https://doi.org/10.23919/IST-Africa67297.2025.11060567

[23] P. Garg, A. Gupta, Y. P. Singh, and P. Goyal. "End-to-End Encryption: Evolution, Barriers, and Emerging Trends", *Deep Quantum Neural Networks: AI for 6G/7G Communication Systems*, pp. 113 - 127, 2026. https://doi.org/10.1007/978-981-95-1683-4_8

[24] P. Baniya, A. Agrawal, K. Abid, J. Nath, B. K. Chaudhary and B. Kunwar, "The Internet of Things: Security Challenges and Opportunities", *2024 3rd International conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC)*, Mathura, India, pp. 153 - 158, 2024. https://doi.org/10.1109/PARC59193.2024.10486356

***