Create a hybrid algorithm by combining Hill and Advanced Encryption Standard Algorithms to Enhance Efficiency of RGB Image Encryption

Rania A. Tabeidi1[1†], Hanaa F. Morse, Samia M. Masaad
Reem H. Al-shammari, Dalia M. Alsaffar
ratabeidi@iau.edu.sa
Computer Department, College of Science and Humanities, Imam Abdulrahman Bin Faisal University P.O.Box 31961, Jubail, Kingdom of Saudi Arabia

Abstract
The greatest challenge of this century is the protection of stored and transmitted data over the network. This paper provides a new hybrid algorithm designed based on combination algorithms, in the proposed algorithm combined with Hill and the Advanced Encryption Standard Algorithms, to increase the efficiency of color image encryption and increase the sensitivity of the key to protect the RGB image from Keyes attackers. The proposed algorithm has proven its efficiency in encryption of color images with high security and countering attacks. The strength and efficiency of combination the Hill Chipper and Advanced Encryption Standard Algorithms tested by statical analysis for RGB images histogram and correlation of RGB images before and after encryption using hill cipher and proposed algorithm and also analysis of the secret key and key space to protect the RGB image from Brute force attack. The result of combining Hill and Advanced Encryption Standard Algorithm achieved the ability to cope statistically

Keywords:
RGB Image, Encryption, Algorithm, AES, Hill

1. Introduction

Recently, with the development of digital devices and the need to send images via the Internet, the importance of information security has emerged [1]. Cryptography is one mechanism used in securing information. There are two types of cryptography, one key encryption, and two key encryptions. The symmetric key encryption is called a private-key scheme, where the secret key not transmitted by the sender and receiver [2,3]. Asymmetric key encryption is called a public-key scheme with two different keys. One of the keys, the public key is available for anyone, the other key is known as the private key [4]. The symmetric cryptosystems security, such as AES, RC4, DES depends on the key size, however, the asymmetric cryptosystems, such as RSA, DSA, and Elliptic Curves depend on the difficulty of the mathematical problem [5]. In a new schema, we propose an algorithm that is a combination of the Advanced Encryption Standard (AES) algorithm and Hill chipper algorithm. AES was adopted by the U.S. government, which is a symmetric key that has a 128-bit block size [6]. The key length of AES cipher is 128, 192, and 256 bits. [7]. Hill cipher was originating in 1929 by the mathematician Lester Hill, it is a multi-letter cipher. Hill cipher is used the secret key that uses matrix size n x n as the key for encryption and decryption [8]. The paper consists of the following: Next section presents the related work on image encryption. Section 3 describes the methodology used to encrypt the images. Section 4 presents the results of the proposed algorithm. Finally, section 5 represents the conclusion.

Manuscript received October 5, 2023
Manuscript revised October 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.10.16

2. Related Work

In [9], the researchers used the Advanced Encryption Standard (AES) Algorithm in the process of encoding and decoding color images by using MATLAB. The result indicates that no information about the image can be obtained after encrypting and the histogram is different between the images before and after encryption. Therefore, the images were successfully encrypted using the mentioned method.

In [10], the researchers combined encryption by using the Advanced Encryption Standard (AES) algorithm and the steganography which is a way to embed secret information. Combining encryption and steganography gives more efficiency when transmission images, especially in the unsecured networks.

In [11], the researchers improved the Hill cipher algorithm to overcome the disadvantages of the algorithm, which consists of not encrypting all the image features with a homogeneous background. The results showed that the proposed algorithm encrypt images with high security and cope the weakness of the original algorithm.

In [12], the researchers combine two methods for encryption namely, Hill Cipher and Caesar Cipher method. They used the proposed method to encrypt the data on exam questions. The method the researchers used relies on one key in the encryption process, which made it simple and easy to understand.

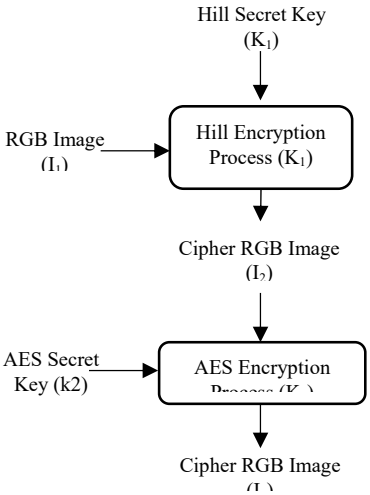
In [13], the proposed algorithm about image encryption based on a secure variant of Hill Cipher (HC) and three improved one-dimensional (1D) chaotic maps. This suggestion algorithm encrypts pixel by pixel in the images. The result showed that the encrypted result by using the proposed algorithm was effective and the time of encryption was short.

In [14], the researchers proposed a new approach to increase the security on the Hill cipher algorithm. They proposed a hybrid encryption algorithm between the elliptic curve cryptosystem and hill cipher (ECCHC). The methodology they proposed converting Hill Cipher from a symmetric technique (private key) to asymmetric one (public key) and increase the security level and efficiency.

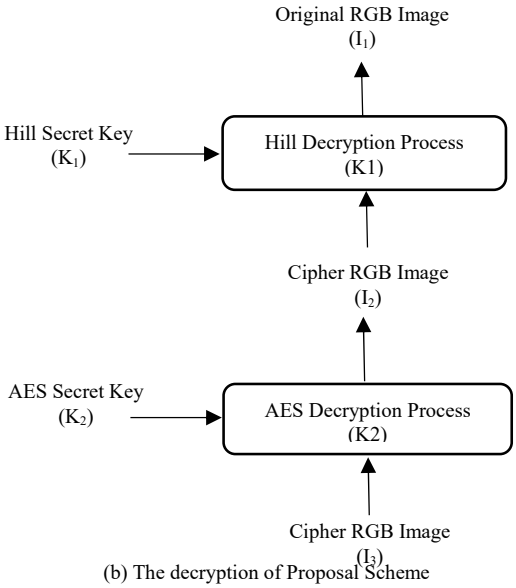
In [15], the researchers proposed a framework to provide security in the cloud. They used two encryption algorithms namely Extended hill cipher and Homomorphic encryption. The first algorithm was applied to encrypt dynamic data while the second algorithm was applied to encrypt static data. The result showed that the proposed algorithm ensures the transmission of information between the cloud and the customer is efficient and safe.

3. Methodology

We proposed a hybrid algorithm by combined the Hill cipher algorithm and Advanced Encryption Standard (AES) cipher algorithm, the Hill cipher inputs are RGB image I_1 and secret key (k_1) contains the secret matrix (K_{2X2}) with two numerical values (C_{2X2}), the output is encrypted RGB image I_2. The RGB image I_2 becomes one of the inputs of the AES cipher with secret key K_2. Figure 1. shows the encryption and decryption of the proposed scheme of hybrid algorithms, in the decryption method, the output encrypted RGB image (I_3) used as the input in Figure 2.

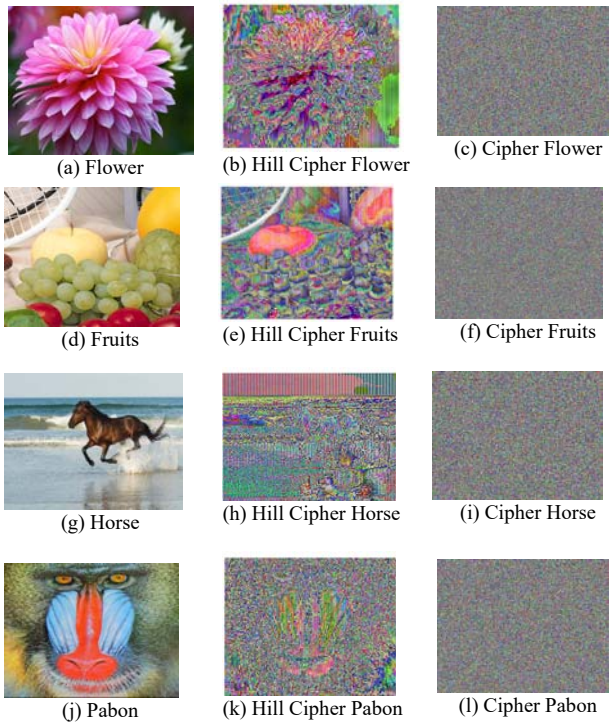


(a) The encryption of Proposal Scheme



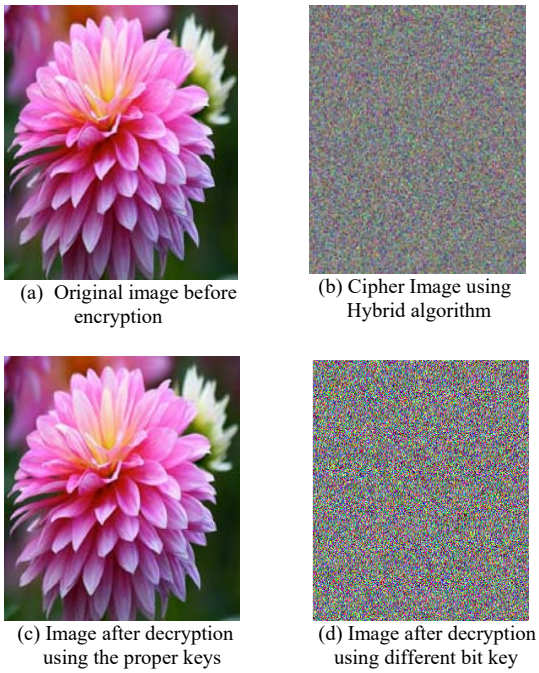
(b) The decryption of Proposal Scheme

Fig 2. The decryption of Proposal Scheme



(a) Flower (b) Hill Cipher Flower (c) Cipher Flower
(d) Fruits (e) Hill Cipher Fruits (f) Cipher Fruits
(g) Horse (h) Hill Cipher Horse (i) Cipher Horse
(j) Pabon (k) Hill Cipher Pabon (l) Cipher Pabon

Fig 2. The plain RGB images and their ciphered RGB image using hybrid algorithm vs Hill cipher



(a) Original image before encryption

(b) Cipher Image using Hybrid algorithm

(c) Image after decryption using the proper keys

(d) Image after decryption using different bit key

Fig 3. The plain RGB images and their ciphered RGB image using Hybrid algorithm and Hill cipher

4. Results

4.1 Security and Performance analysis

We used MATLAB 2020 to analyze several properties of the image before and after encoding, four images were used for encryption and decryption.

4.1.1 Analysis of Key Space

Try to find the secret key used to decrypt the message, as it depends on the number of attempts, which is directly proportional to a key space. In the proposed algorithm, along the key (256 bits, 2^{256} area with 2^{256} Attempts) was used sufficiently to protect the color image from this type of attack.

4.1.2. Analysis of secret Key

The key sensitivity means the change ratio of the cipher-image pixels if a slight bit of the key is changed. Also, shows the effectiveness of changing only one bit key, or choosing the wrong key lead to a different result for obtaining the corresponding plain image. Figure 3 shows the differences between the two ciphered images for two identical images with only one difference bit. It is shown there is a full difference between two ciphered images.

4.2 Statical analysis

Most cipher algorithms are broken using statistical analyzes. Analyzes are used to find a linkage between the cipher and the original images to gain access to the secret key, to overcome statistical attacks the publishing and disturbance features of the cipher algorithm must be available. The following statistical analyzes were performed for the encrypted image:

4.2.1 Histogram Analysis

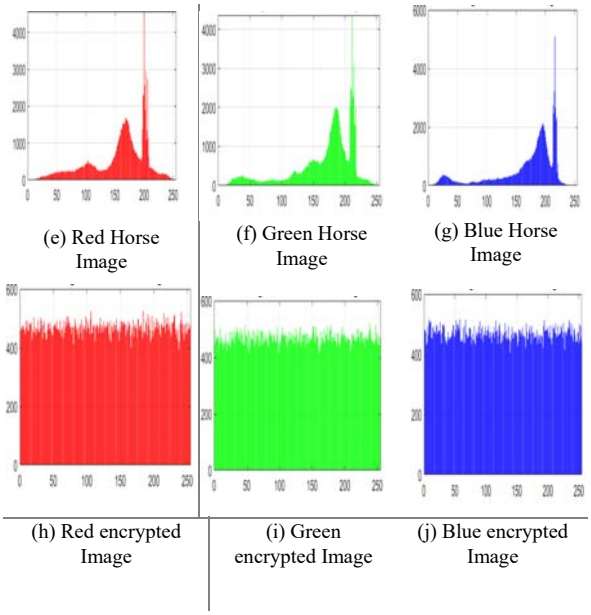
It indicates how the values of the RGB image's pixels are distributed by drawing the number of times values are repeated different from the histogram of the plan image. Figure 4 shows the histogram of the flower plain red, green, and blue images and the corresponding ciphered images are shown in Figure.5 histograms of the cipher RGB image are different from the plain image histogram and uniform.

(a) Plain Horse Image

(b) Red Horse Image

(c) Green Horse Image

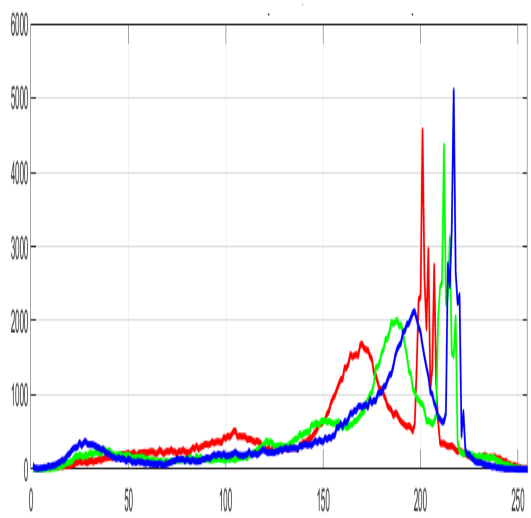
(d) Blue Horse Image



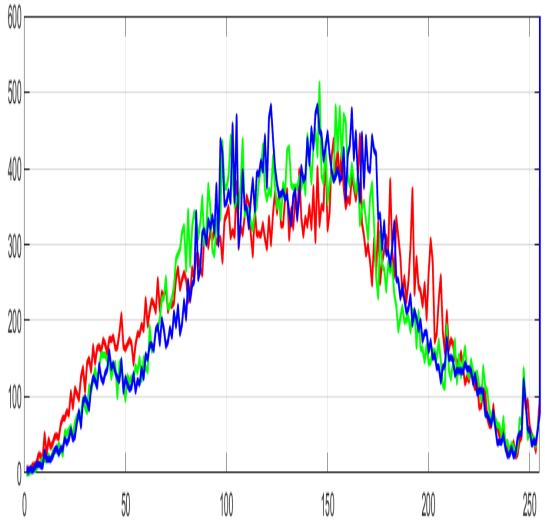
(e) Red Horse Image (f) Green Horse Image (g) Blue Horse Image

(h) Red encrypted Image (i) Green encrypted Image (j) Blue encrypted Image

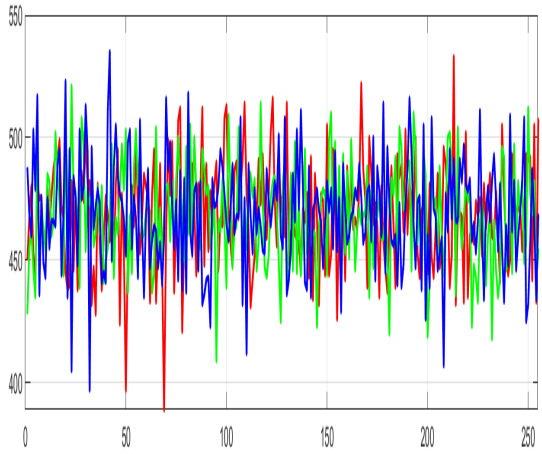
Fig 4. (e-g) Histogram of RGB plain image (h-j) Histogram RGB corresponding cipher image



(a) RGB image



(b) Original Hill RGB Image Histogram



(c) Proposed Cipher RGB Image Histogram

Fig 5. The histogram of (a) RGB image, (d)Original Hill RGB image, and (c) Proposed cipher RGB image

4.2.2 Correlation between original and cipher images

If the coefficient of correlation is close to zero, the correlation between the image after and before encryption decreases, and there's difficulty extract the original image [16]. When comparing the correlation coefficient using the Hill algorithm as in Table 1 and Table 2 and the proposed algorithm in Table 3 and Table 4 notice the strength of the proposed schema.

Table 1. Red, green, and blue of plain and cipher image for Hill Algorithm correlation

Image Name	***Flower***	***Fruits***	***Horse***	***Baboon***
Size	392*512*3	512*512*3	300*400*3	512*512*3
C_{RR}	0.1942	0.37708	0.55843	0.47476
C_{GG}	0.45205	0.28527	0.51348	0.53106
C_{BB}	0.27087	0.36954	0.50823	0.40563
C_{RG}	0.14352	0.31644	0.52559	0.46167
C_{RB}	0.17845	0.28964	0.53971	0.45781
C_{GR}	0.45951	0.30927	0.54613	0.5166
C_{GB}	0.45262	0.25707	0.52117	0.52012
C_{BR}	0.2696	0.35839	0.53494	0.40598
C_{BG}	0.2577	0.38944	0.50559	0.42377

Table 2. Red, green, and blue of plain and cipher image for proposed Algorithm correlation

Image Name	***Flower***	***Fruits***	***Horse***	***Baboon***
Size	392*512*3	512*512*3	300*400*3	512*512*3
C_{RR}	-0.00034	0.00036	0.00189	0.00303
C_{GG}	-0.00226	-0.00118	0.00506	0.00601
C_{BB}	-0.00003	-0.00137	0.00051	0.00399
C_{RG}	-0.0033	-0.00252	0.00453	0.00396
C_{RB}	-0.00062	-0.00231	0.00183	-0.00146
C_{GR}	-0.00193	-0.00142	0.00135	0.0045
C_{GB}	0.00133	0.00077	0.00191	-0.00046
C_{BR}	-0.00122	0.00091	0.00161	0.00204
C_{BG}	-0.00149	-0.00076	0.00382	0.0074

5. Conclusion

We proposed an asymmetric hybrid algorithm; Hill cipher and Advanced Encryption Standard Algorithms were joined to propose a new encryption algorithm to encrypt color images. The results showed that the proposed system was able to encode color images with high efficiency against attacks. The encryption key was used to encrypt the images, therefore increasing the key strength to counter attacks and statistical attacks. The results showed that encrypting the images using the proposed schema is more secure and effective than the original one. The combination of both algorithms has been successfully applied to RGB images of different size.

References

[1] Xingyuan Wang, Hui-li Zhang, Madhuviswanatham, A. V. N. Krishna, A color image encryption with heterogeneous bit -permutation and correlated chaos 2014 Elsevier

[2] Y. Li, F. Zhang, Y. Li, et al., Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform, Opt. Lasers Eng. 72 (2015)18–25

[3] J. Daemen and V. Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard J. Springer-Verlag. 2002:55-56).

[4] S. Kartalopoulos, "Security of Information and Communication Networks", Wiley-IEEE Press, (2009).

[5] Priyadarshini Patil, Prashant Narayankar, Narayan D G, Meena S Md, A Comprehensive Evaluation of Cryptographic Algorithms: DES,3DES, AES, RSA,Blowfish. (2016) 617 – 624

[6] Hongjun Liu, Abdurahman Kadir, Yangling Li, 'Asymmetric color image encryption scheme using 2D discrete-time map (2015)104–112

[7] KOCAREV L, Lian S, editors. Chaos based cryptography. Springer; 2011

[8] K. Adinarayana Reddy, B. Vishnuvardhan, Madhuviswanatham, A. V. N. Krishna,'A Modified Hill Cipher Based on Circulant Matrices Procedia TechnologyVolume 42012Pages 114-118

[9] Zhang, Q., & Ding, Q. (2015, September). Digital image encryption based on advanced encryption standard (aes). In 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC) (pp. 1218-1221). IEEE.

[10] Reddy, M. I. S., & Kumar, A. S. (2016, January). Secured data transmission using wavelet based steganography and cryptography by using AES algorithm. In Elsevier, International Conference on Computational Modeling and Security (CMS), Procedia Computer Science (Vol. 85, pp. 62-69).

[11] Hraoui, S., Gmira, F., Abbou, M. F., Oulidi, A. J., & Jarjar, A. (2019). A new cryptosystem of color image using a dynamic-chaos Hill Cipher algorithm. Procedia computer science, 148, 399-408.

[12] Agung, A., Heryana, N., & Solehudin, A. (2020). Combination of Hill Cipher Algorithm and Caesar Cipher Algorithm for Exam Data Security. Buana Information Technology and Computer Sciences (BIT and CS), 1(2), 42-45.

[13] Essaid, M., Akharraz, I., & Saaidi, A. (2019). Image encryption scheme based on a new secure variant of Hill Cipher and 1D chaotic maps. Journal of Information Security and Applications, 47, 173-187.

[14] Almaiah, M. A., Dawahdeh, Z., Almomani, O., Alsaaidah, A., Al-khasawneh, A., & Khawatreh, S. (2020). A new hybrid text encryption approach over mobile ad hoc network. International Journal of Electrical and Computer Engineering (IJECE), 10(6), 6461-6471.

[15] Das, B. K., & Garg, R. (2019, July). Security of Cloud Storage based on Extended Hill Cipher and Homomorphic Encryption. In 2019 International Conference on Communication and Electronics Systems (ICCES) (pp. 515-520). IEEE.

[16] N. El-Fishawy and O. Zaid, "Quality of encryption measurementof bitmap images with rc6, mrc6, and rijndael block cipher algorithms," International Journal of Network Security, vol. 5,

[17] Arab, A., Rostami, M. J., & Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. *The Journal of Supercomputing, 75*(10), 6663-6682. doi:10.1007/s11227-019-02878-7