RGB Image Encryption using Hill Algorithm and Chaos System

Ali Jawad Ibada\textsuperscript{1,2}, Phaklen Ehkan\textsuperscript{2,3}, Ruzelita Ngadiran\textsuperscript{2,3}, Dalal Abdulmohsin Hammood\textsuperscript{1,4}, Ahmed Alkhayyat\textsuperscript{4}

\textsuperscript{1}College of Engineering, Islamic university, Najaf, Iraq
\textsuperscript{2}Centre of Excellence Advanced Computing (ADVCOMP), Universiti Malaysia Perlis (UniMAP), 02600 Arau, Perlis, Malaysia
\textsuperscript{3}Faculty of Electronic Engineering Technology, Universiti Malaysia Perlis (UniMAP), 02600 Arau, Perlis, Malaysia
\textsuperscript{4}Electrical Engineering Technical College, Middle Technical University (MTU), Al Doura 10022, Baghdad, Iraq

*Correspondences: phaklen@unimap.edu.my; dr.ahmedalkhayyat85@gmail.com

Abstract. The development of modern technology in recent years, makes the data security very big issue. To secure our data from unauthorized person, encryption is used before transmission. Various sensitive information is using encryption such as: e-mail messages, banking transactions, credit information and military operations. The encrypted data can be in form of text, image, voice, and video. In this paper, a proposed Hill algorithm with chaos system is used to encrypt colour RGB (Red, Green and Blue) image. The key of Hill algorithm is a square matrix. The selection of matrix key numbers is very important. Therefore, chaos system is used to generate sequences of numbers for Hill key matrix. These sequences have a property of randomness that make it very difficult for guessing. Finally, the proposed system is simulated using MATLAB, and a test image is encrypted and decrypted using proposed system successfully.

1. Introduction
Every transmitted data over networks can be suffer an attack by third party. Therefore, cryptography is used to secure data from unauthorized person. Cryptography is an art and science of hiding data from the external environment. It is basically classified into two categories: symmetric cipher and asymmetric cipher [1-2]. In a symmetric cipher, both sender and receiver used same shared key (such as Hill cipher). While in asymmetric cipher, there are two keys. The first key is a public key that is used by the sender to encrypt message, while the second key is a private key that is used by the receiver to decrypt message (such as RSA cipher). Encryption is a process to convert the original message to encrypt message using a specific key. While decryption is the reverse process of encryption, it is retrieving the original message from encrypted message [3]. The original message can be any transmitted data such as text or image. Colour images are being transmitted and stored over networks, which take advantage of rapid development in multimedia and network technologies. Image encryption has applications in different fields such as multimedia systems, internet communication, medical imaging, and military communication [4]. In recent years, some papers were proposed encryption using chaos system [5-12]. The attractiveness of using chaos is that it has the properties which are very sensitive to initial condition, long term unpredictable sequence, and the implementation of hardware and software is simple [13]. Some researchers were also using Hill cipher algorithm [14-15]. In this paper, a colour image is encrypted using both chaos system and Hill cipher so that each colour in RGB image is encrypted separately and then combined.
for transmission. Finally, the proposed method in this work is simple and efficient to encrypt and secure colour images.

2. Hill Cipher Algorithm

The principle of Hill cipher algorithm based on linear algebra properties. It uses square matrix Key (K) modulo 26 (there are 26 English letters). The inverse of K (K⁻¹) must be exist to satisfy decryption process [3] [16]. This means that:

\[ K \cdot K^{-1} \mod 26 = I \]  

(1)

where, I is identity matrix. Each English letter takes numerical value, so that a = 0, b = 1, c = 2, …, z = 25. In encryption process, plain-text (P) letters are subdivided into several segments. The length of each segment equals to K rows (or column). The encryption equation that generate Cipher-text (C) is shown as follow:

\[ C = E(K, P) = K \cdot P^T \mod 26 \]  

(2)

where, E is encryption process and \((T)\) is transpose operation. While the decryption equation is:

\[ P = D(K, C) = K^{-1} \cdot C^T \mod 26 \]  

(3)

3. Chaos System

Chaos is aperiodic, random-like, long term non-predictive behaviour, and very sensitive to initial condition [17]. The chaos sequence is implemented using several chaotic maps. Any chaotic map is defined as [18]:

\[ y_{n+1} = f(y_n), n = 0, 1, 2, \ldots \]  

(4)

where, \(y_{n+1}\) is the present value of \(y\) and \(y_n\) is the previous value. Several chaotic maps are existing, such as logistic map, Lorenzo map, and quadratic map. Logistic map is used in this work that is given by:

\[ y_{n+1} = y_n \cdot r \cdot (1 - y_n) \]  

(5)

where, \(r\) is bifurcation parameter which lies between [0,4].

Fig. 1 shows the bifurcation diagram of the logistic map. From this figure, it is shown that chaotic behaviour occurs when \(r\) is between [3.68, 4].

![Bifurcation diagram of logistic map](image)

Fig. 1. Bifurcation diagram of logistic map

Fig. 2 shows the concept of logistic map sensitivity to the initial conditions. Two sequences are generated in this figure; one with \(y_0 = 0.1\) and the other with \(y_0 = 0.10001\). After 15 iterations, it can be seen that the two sequences are entirely different. In fact, as the length of the sequence is increase, the randomness is increase in it as well.
4. Proposed Encryption Algorithm

In this work, RGB image is encrypted by combining Hill cipher and chaos system. RGB image contains of three colour matrices which include R matrix, B matrix, and G matrix. The pixel size in each colour matrix is 8-bits which is $2^8 = 256$. So, all operations are based on modulo 256. The next sections will state the encryption and the decryption processes of the proposed method.

A. Encryption process

The steps of RGB image encryption include:

1) Three different initial condition values are chosen to generate three chaos sequences. In this paper, the initial conditions that used are 0.1578249875, 0.4904128756, and 0.8361527407 values. The length of each sequence is 10000. The increasing of sequence length leads to increase the randomness of numbers. All generated numbers are lie between [0,1]. For this reason, all generated numbers are multiplied by 1000, then rounded to nearest integer value.

2) Any 16 values of each sequence are taken to create 4*4 Hill matrix keys (K1, K2, and K3) as follow:

\[
\begin{bmatrix}
18 & 209 & 254 & 175 \\
69 & 36 & 246 & 92 \\
1 & 118 & 223 & 226 \\
252 & 164 & 12 & 231 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
219 & 179 & 32 & 130 \\
50 & 200 & 51 & 197 \\
190 & 128 & 80 & 223 \\
103 & 154 & 198 & 35 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
216 & 115 & 250 & 139 \\
23 & 166 & 214 & 80 \\
149 & 247 & 27 & 125 \\
128 & 232 & 140 & 127 \\
\end{bmatrix}
\]

K1 is used to encrypt R matrix, while K2 is used to encrypt G matrix and K3 is used to encrypt B matrix. All key matrices are achieved Hill cipher conditions to generate $K^{-1}$ modulo 256, so that $K \times K^{-1}$ modulo 256 = I.

3) Each colour matrix is subdivided into several 4*4 segments. After that, each segment is multiplied with its specific K to generate encrypted matrix.

4) All encrypted matrices are combined together to create encrypted image that is transmitted over network.
B. Decryption process

Both sender and receiver are used the same initial conditions. Therefore, receiver calculate the inverse of Hill matrix keys ($K_1^{-1}$, $K_2^{-1}$, and $K_3^{-1}$). The decryption process is:

1) When the encrypted image reach at the receiver, it is separated to three encrypted matrices, each matrix is belonging to one colour of RBG image.

2) Each encrypted matrix is subdivided into several 4*4 segments. Then, each segment is multiplied with its specific $K^{-1}$ to get R, B and G matrices.

3) All R, B and G matrices are combine together to retrieve the original RBG image.

All steps of encryption and decryption process flow are clearly shown in Fig. 3.

5. Results

The proposed algorithm is simulated using MATLAB program. The original test image with its histogram is shown in Fig. 4. Fig. 5 displays the R, G and B of the original test image independently. While Fig. 6 demonstrates the encryption of each colour image separately. Lastly, the final encryption step is combining all three encryption colours together as shown in Fig. 7.
Fig. 4. Original test image and its histogram

Fig. 5. Red, Green and Blue images of the original image

Fig. 6. The encryption of R, G and B image

Fig. 7. Encrypted image with its histogram
When the encrypted image is received, the original image can be retrieved by doing the reverse process of all encryption steps. Fig. 8 shows the decrypted image in the receiver which similar to the original image in the Fig. 4.

![Decrypted Image](image)

**Fig. 8.** Decrypted image with its histogram

### 6. Conclusion

In this paper, a proposed method is used to improve Hill cipher algorithm by using chaos system. RGB image can be encrypted using the proposed method which is simple to be implemented and efficient. Each colour of image is encrypted individually using different key so that, each key is created from different chaos sequence. These chaos sequences are generated using initial conditions which are entirely different from each other. In fact, the chaos sequence has a property of dependency on initial condition. This makes a small change in the initial condition will create entirely different chaos sequence. Therefore, the attacker will face several difficulties such as 1) the estimation of three initial conditions of chaos system which is very sensitive and difficult, 2) each colour of RGB image is encrypted alone, this makes confusion of which initial condition is used to each colour, 3) the size of Hill matrix key, which set the size of segments during encryption and decryption process, 4) the selection of Hill matrix key numbers from millions of numbers in the generated chaos sequences. Simulation results show that, the encryption of any image is entirely hidden by using the proposed algorithm.

### Acknowledgement

The authors would like to gratefully acknowledge the Ministry of Higher Education, Malaysia who provide the financial support for this work under the Fundamental Research Grant Scheme, FRGS/1/2020/ICT02/UNIMAP/02/5.

### References

[1] Dorothy Denning, Cryptography and data security. USA: Addison-Wesley, 1982.
[2] Himanshu Gupta, Designing some multiple and multiphase encryption techniques for the enhancement of data security.: Haridwar, 2014.
[3] William Stallings, Cryptography and network security: principles and practice, Sixth ed. New Jersey, USA: Pearson Education, 2014.
[4] Ming-Jheng Li, Yi-Chun Wang, Justie Su-Tzu Juan Joy Jo-Yi Chang, "Two-image encryption by random grids," 10th International Symposium on Communications and Information Technologies, pp. 458-463, 2010.

[5] Yaobin Mao, Charles K. Chui Guanrong Chen, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, solitons and fractals, vol. 21(3), pp. 749–761, 2004.

[6] Fangjun Huang, Wenjie Guan Zhi-Hong Guan, "Chaos-based image encryption algorithm," Physics letters A, vol. 1 (3), pp. 153–157, 2005.

[7] Vinod Patidar, K.K. Sud N.K. Pareek, "Image encryption using chaotic logistic map," Image and vision computing, vol. 24 (9), pp. 926–934, 2006.

[8] Zengqiang Chen Tiegang Gao, "A new image encryption algorithm based on hyper-chaos," Physics Letters A, vol. 372 (4), pp. 394–400, 2008.

[9] Xiaofeng Liao, Pengcheng Wei Di Xiao, "Analysis and improvement of a chaos-based image encryption algorithm," Chaos, solitons and fractals, vol. 40 (5), pp. 2191–2199, 2009.

[10] Wei Zhang, Kwok-wo Wong, Hai Yu Zhi-liang Zhu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," Information sciences, vol. 181 (6), pp. 1171-1186, 2011.

[11] Kwok-Wo Wong, Xiaofeng Liao, Guanrong Chen Yong Wang, "A new chaos-based fast image encryption algorithm," Applied soft computing, vol. 11 (1), pp. 514–522, 2011.

[12] Lin Teng, Xue Qin Xingyuan Wang, "A novel colour image encryption algorithm based on chaos," Signal processing, vol. 92 (4), pp. 1101-1108, 2012.

[13] Bruce Schneier, Applied cryptography: protocols, algorithms, and source code in C, Second ed, New york, USA: Wiley, 1996.

[14] Naveen Kumar S K Panduranga H. T., "Advanced partial image encryption using two-stage hill cipher technique," International journal of computer applications, vol. 60 (16), pp. 14-19, 2012.

[15] A.F.A., O.Y. Chuan and M.R.K. Ariffin Abidin, "A novel enhancement technique of the hill cipher for effective cryptographic purposes," Journal of computer science, vol. 7(5), pp. 785-789, 2011.

[16] Mohsen Toorani and Abolfazl Falahati, "A secure variant of the Hill Cipher," in 2009 IEEE symposium on computers and communications, Sousse, Tunisia, pp. 313-316, 2009

[17] Stephen Wiggins, Introduction to applied nonlinear dynamical systems and chaos, Second ed. New York, USA: Springer-Verlag, 2003.

[18] S. Azou, G. Burel, and C. Pistre, "A chaotic Direct-sequence spread-spectrum system for underwater communication," in Oceans '02 MTS/IEEE, Biloxi, MI, USA, pp. 2409-2415, 2012.