Optics and Laser Technology 95 (2017) 94–99

Contents lists available at ScienceDirect

Optics and Laser Technology

journal homepage: www.elsevier.com/locate/jolt

Full length article

# Cryptanalysis of an image encryption algorithm based on DNA encoding

A. Akhavan [a,*], A. Samsudin [a], A. Akhshani [b]

[a] School of Computer Sciences, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia
[b] Department of Physics, Urmia Branch, Islamic Azad University, Urmia, Iran

ARTICLE INFO

*Article history:*
Received 8 August 2016
Received in revised form 12 March 2017
Accepted 19 April 2017
Available online 6 May 2017

*Keywords:*
Cryptanalysis
DNA encoding
Image encryption
Shuffling
Security
Chosen plaintext attack

ABSTRACT

Recently an image encryption algorithm based on DNA encoding and the Elliptic Curve Cryptography (ECC) is proposed. This paper aims to investigate the security the DNA-based image encryption algorithm and its resistance against chosen plaintext attack. The results of the analysis demonstrate that security of the algorithm mainly relies on one static shuffling step, with a simple confusion operation. In this study, a practical plain image recovery method is proposed, and it is shown that the images encrypted with the same key could easily be recovered using the suggested cryptanalysis method with as low as two chosen plain images. Also, a strategy to improve the security of the algorithm is presented in this paper.



## 1. Introduction

During the past decade, the rapid growth of the Internet and application of digital media such as images and video has motivated numerous researchers in the field of cryptography to propose encryption algorithms specific for digital media and particularly images [1–5]. The motivation has usually been bulk data in the images and difficulty of encrypting images without any apparent pattern of the plain image in the ciphered image [6]. Thus, the researchers in this field aimed to improve the randomness of the generated ciphertext in order to achieve a robust image encryption algorithm without any obvious pattern in the ciphered image [6]. The required randomness was usually obtained from conventional methods based on chaotic maps such as tent map [7], logistic map [8], trigonometric chaotic maps [9], CAT and Baker map [10], coupled map lattice [11], Quantum chaos [12], Jacobian elliptic maps [13], Polynomial [14], Hyper-chaotic [15] and high dimensional chaotic maps [16].

In addition, several DNA coding based random sequence generators have been used to diffuse and confuse the pixel values in image encryption algorithms [17–21]. However, some of these algorithms have been found weak against differential cryptanalysis, for instance, Xie et al. [22] cryptanalyzed a DNA-based image encryption with as few as three chosen plain images and also Liu et al. [23] that cryptanalyzed a DNA-based RGB image encryption algorithm using known plaintext attack.

In the current study also, security of an image encryption algorithm based on DNA-coding and Elliptic Curve DiffieHellman Encryption (ECDHE) for key exchange is investigated [24]. In this paper, the main goal is to find a universal method to decrypt the ciphered image, without access to the keys. Therefore, the key exchange method described for sharing keys between sender and receiver is not in the scope of the analysis, and the main focus is to recover the plain image. The results of the security analysis show that the algorithm presented in [24] is not strongly dependent on the keys and regardless of the selected keys, the overall pixel values remain the same and are just shuffled. Thus the current attack, is similar to other attacks proposed on shuffling based image encryption algorithms [6,25–27]. The other disadvantage of the proposed image encryption algorithm is the low entropy of the randomness source. The so-called DNA coding methods, in nature, is only a 2-bit grouping strategy. In classic bit based image encryption algorithms, each pixel of the image is decomposed to the constructing 8-bit binary representation. Similarly, in this method, the pixels are divided into composing 2-bit elements. As the presence of three layers of colors only increase the complexity of the cryptanalysis and do not participate in improving the security of the image encryption algorithm, initially the algorithm is cryptanalyzed using the gray-scale image and then the steps are generalized over the three colors. In addition to the previously described drawbacks, the image encryption algorithm under study [24] can be cryptanalyzed with access to only two chosen plain images, which makes it immensely insecure against chosen plaintext attack. In this paper, a simple method for cryptanalysis of [24] is

* Corresponding author.
*E-mail address:* amir.akhavan@yahoo.com (A. Akhavan).

http://dx.doi.org/10.1016/j.optlastec.2017.04.022
0030-3992/

presented in Section 3. The rest of this paper is organized as follows. Section 2 revisits the algorithm under study.

The rest of this paper is organized as follows. In Section 2, the image encryption algorithm under study is described. In Section 3, the proposed cryptanalysis method is described, and as a case study, sample images are encrypted and decrypted with the algorithms proposed in [24].

## 2. Image encryption algorithms under study

The structure and steps of the DNA based image encryption algorithm proposed in [24], is reviewed in this section. The figures related to the image encryption are the same figures used in the original paper to exactly reflect the process of the encryption. The image encryption algorithms which is under study in this paper consists of the following steps: The proposed algorithm in [24], is a RGB color image encryption algorithm. In this section the steps of the algorithm as defined in the paper are mentioned and each step is reviewed. First the plain-image, which in nature is a RGB image, is decomposed into the constructing layers. The constructing layers each contain 8-bit pixels, which are transformed into 2-bit DNA representations ($00-A$, $11-T$, $01-C$, and $10-G$). Then the layers are scrambled by the DNA addition table (see Table 1). The 'addition step', the method used in the proposed algorithm, is only a static shifting procedure and can be reversed with no effort and requirement to the keys.

Following the DNA addition, the circular shifting of the image is conducted using the method provided in Fig. 1. It is claimed that, the Circular shifting is performed in order to "distort the correlation of the pixel values by scrambling them independently in the spatial domain" [24]. In addition, the length of shifting sequence can be selected based on the required security. The shifting amount is identified by using the private keys between the parties ($K_R, K_G$ and $K_B$), which are shared using Elliptic curve DiffieHellman key exchange method. Following shifting, the Red, Green and Blue layers are "interleaved to increase the variation in the correlation of the image across the layers in spatial domain" [24] (see Fig. 2). The key exchange procedure is carried on to share three private keys each one for one image layer. The process of the encryption is shown in Fig. 3, and described in steps as below:

Steps 1: The RGB image $I(m \times n \times 3)$, is imported.

Steps 2: The pixels are transformed into their DNA symbolic representation (2-bit) and placed into a 3D matrix of DNA codes.

Steps 3: The DNA addition operation is applied on all the elements of matrix using the following equations: $R_{DNA}(i,j) = R(I,j) + G(i,j)$
$G_{DNA}(i,j) = G(i,j) + B(i,j)$
$B_{DNA}(i,j) = G_{DNA}(i,j) + B(i,j)$

Steps 4: Each of the layers (dimensions of matrix) undergoes a circular shift operation using the values given by ECDHE keys and the direction provided in Fig. 1.

Steps 5: The rows of matrix are substituted similar to RRRGGGBBB interleaved as RGBRGBRGB (see Fig. 2).

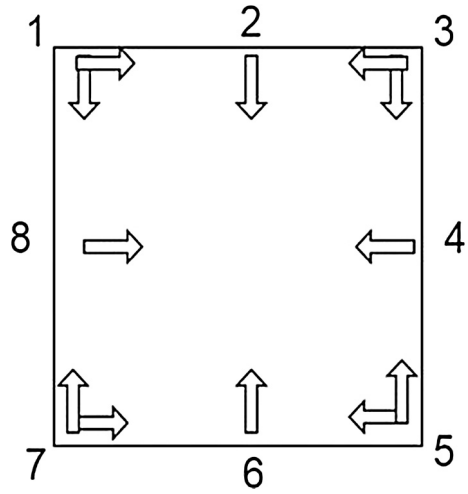


**Fig. 1.** Process of shifting: 1-Down and right; 2-Down; 3-Down and left; 4-Left; 5-Up and left; 6-Up; 7-Up and right; 8-Left. (Provided in [24].)

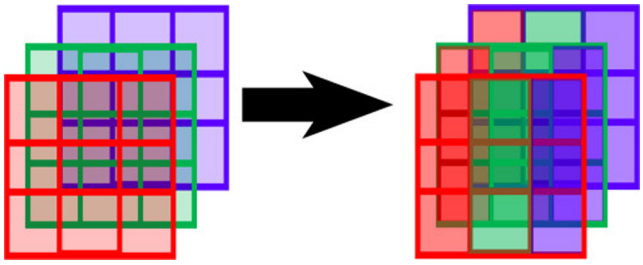

**Fig. 2.** Interleaving of an RGB image. (Provided in [24].)

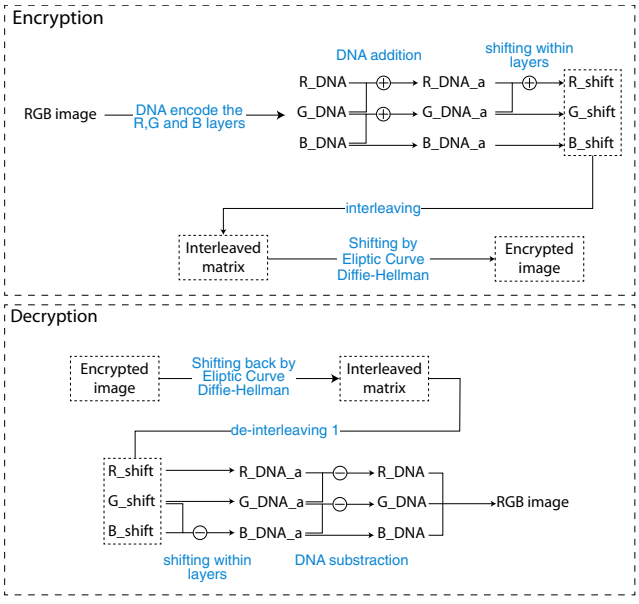


**Fig. 3.** Flowchart of the proposed algorithm. (a) Encryption. (b) Decryption. (Provided in [24].)

**Table 1**
Addition and subtraction rule for DNA given in [24].

| + | A | T | C | G | − | A | T | C | G |
|---|---|---|---|---|---|---|---|---|---|
| G | G | C | T | A | G | G | T | C | A |
| C | C | A | G | T | C | C | G | A | T |
| T | T | G | A | C | T | T | A | G | C |
| A | A | T | C | G | A | A | C | T | G |

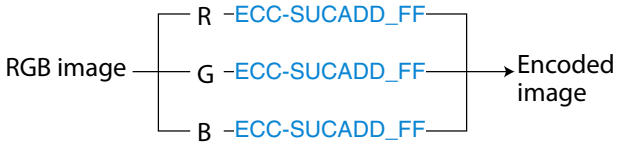


**Fig. 4.** ECC-SUCADD-FF: Elliptic curve cryptography using successive addition over finite field. (Provided in [24].)

Steps 6: In this step, the ECDHE operation is conducted. In this step the variables $R_{DNA}, G_{DNA}$, and $B_{DNA}$ are the DNA encoded values of the red, green and blue pixel values of the RGB image (left column of Fig. 3) that are shifted (shuffled) using $X_r, Y_r, X_g, Y_g, X_b$, and $Y_b$ (fixed shared values generated by ECDHE) $R_{DNA} \times (X_r, Y_r)$ over $E_R(a_{1r}, a_{2r}, a_{3r}, a_{4r}, a_{6r})$,
$G_{DNA} \times (X_g, Y_g)$ over $E_G(a_{1g}, a_{2g}, a_{3g}, a_{4g}, a_{6g})$,
$B_{DNA} \times (X_b, Y_b)$ over $E_B(a_{1b}, a_{2b}, a_{3b}, a_{4b}, a_{6b})$.
Fig. 4 is presented in the paper to demonstrate how the encryption mentioned above operates.

Steps 7: The RGB components are again interleaved.

Steps 8: Finally, RGB components are recombined to get the encrypted image.

The steps described earlies, are applied in a numerical study, which clarifies process of some of the sections.

## 3. Cryptanalysis

The presented image encryption algorithm, is claimed to be secure because of using DNA-coding and ECDHE. However, the experimental results provided in the security analysis section, provides sufficient evidence to suggest that the image encryption algorithm presented in [24] is a shuffling only encryption. In the other words, the pixel values plain image $I(m \times n \times 3)$ and the final cipher image $C(m \times n \times 3)$ are the same with different locations. The simulation results of [24] is shown presented in Fig. 5.

The black image (j in Fig. 5), and the corresponding cipher image (k in Fig. 5), are both exactly the same. In addition, (h in Fig. 5) is the encrypted value of (g) in Fig. 5. The uniform distribution of visible pattern in encrypted image (g) also indicates that all the pixels with value of ($R = 255$, $g = 255$, $b = 255$) are left untouched.

With this hypothesis that the image encryption algorithm in [24] is a shuffling only algorithm, and by considering the general requirements of analysis of a shuffling only image encryption described in [6], only $Log_{255}(2mn - 1)$ known plain images are required to regenerate the inverse permutation matrix ($W^{-1}$). In [6], the shuffling only encryption algorithm is assumed to have a permutation matrix $\mathbf{W} = [w(i,j) = (i',j') \in M \times N]_{M \times N}$. However, the number of required chosen plain images is still too much, whereas in the next section it will be shown that the reveres permutation map $\mathbf{W}^{-1}$ can be generated using only two chosen plain images and their corresponding ciphered images.

### 3.1. Chosen-plaintext attack

In this section the image encryption algorithm is revisited and implementation steps are described to perform the cryptanalysis task. According to Kerckhoff's principle it is assumed that a third party (Eve) has access to the encryption and decryption algorithm, but not to the shared keys exchanged using the ECC based Diffie-Hellman key exchange method. The two chosen plain images (for each layer) in the process of cryptanalysis of the algorithm are $P_1$ and $P_2$ with the size of $256 \times 256$ pixels. The chosen plain image $P_1$ is a RGB image (three layers of R, G and B) where in each row, in each layer, the pixel values grow from 0 to 255. Thus, the image looks like a horizontal gradient of colors. Similarly, but in vertical direction the pixel values of $P_2$ grow from 0 to 255. Therefore, the chosen plain image $P_2$ looks like a vertical gradient of colors. Meanwhile, the corresponding cipher images for the chosen plain images $P_1$ and $P_2$ are named as $C_1$ and $C_2$ respectively. In order to reduce the complexity of the cryptanalysis the following steps are conducted on the proposed algorithm in Section 2.

Phases 1: In step 7 of the algorithm proposed in 2, the pixel values are interleaved. However, this interleaving process can be undone without required access to any key. Therefore in the first step, both $C_1$ and $C_2$ are de-interleaved back to the condition in step 6 (from steps in 2).

Phases 2: In step 5 (from steps in 2), the pixels are again interleaved with simple substitution of the columns as shown in 2. The process also can be undone without access to the keys, therefore, both $C_1$ and $C_2$ are again de-interleaved. The final outcomes are stored in $M_1$ and $M_2$ (M stands for medial values).

Phases 3: In step 3 (from steps in 2) the DNA addition operation is applied on the plain image, the similar operation can be reversed with access to the DNA subtraction table (Table 1). For the purpose of simplicity, the DNA subtraction step is also undone to avoid any confusion between the steps. However, it was also possible to ignore effect of this step only by assigning 0 to the pixel values of 2 layers (for instance Blue and Green) and limiting the operation on one layer (Red).

Phases 4: In this phase, two new matrices for storing the permutation map are generated ($\mathbf{V}_{256\times256\times3}$ and $\mathbf{H}_{256\times256\times3}$). The matrix $\mathbf{V}$ stores the vertical disposition of the pixels and $\mathbf{H}$ stores the Horizontal disposition.

Phases 5: The layer of $M_1(i,j,k)$ are individually compared with $P_2(i,j,k)$, using a simple column comparison procedure. For each layer the following code is operated.

```
for k = 1 : 3 do
    for i = 1 : 256 do
        for j = 1 : 256 do
            V(i,j,k)=M1(i,j,k)+1;
            H(i,j,k)=M2(i,j,k)+1;
        end for
    end for
end for
```

Phases 6: The horizontal disposition matrix ($V(i,j,k)$) and vertical disposition matrix ($H(i,j,k)$) combined together are the reverse shuffling map of the encryption algorithm. Having access to these two matrices it is possible to reverse the position of the pixels in any ciphered image and achieve to the corresponding plain image.

### 3.2. Simulation

In order to practically experiment the cryptanalysis using chosen plain image attack, first the permutation matrices are regenerated as described in Section 3.1. Then, the generated matrices are applied to decrypt ciphered images Figs. 7 and 8, without access

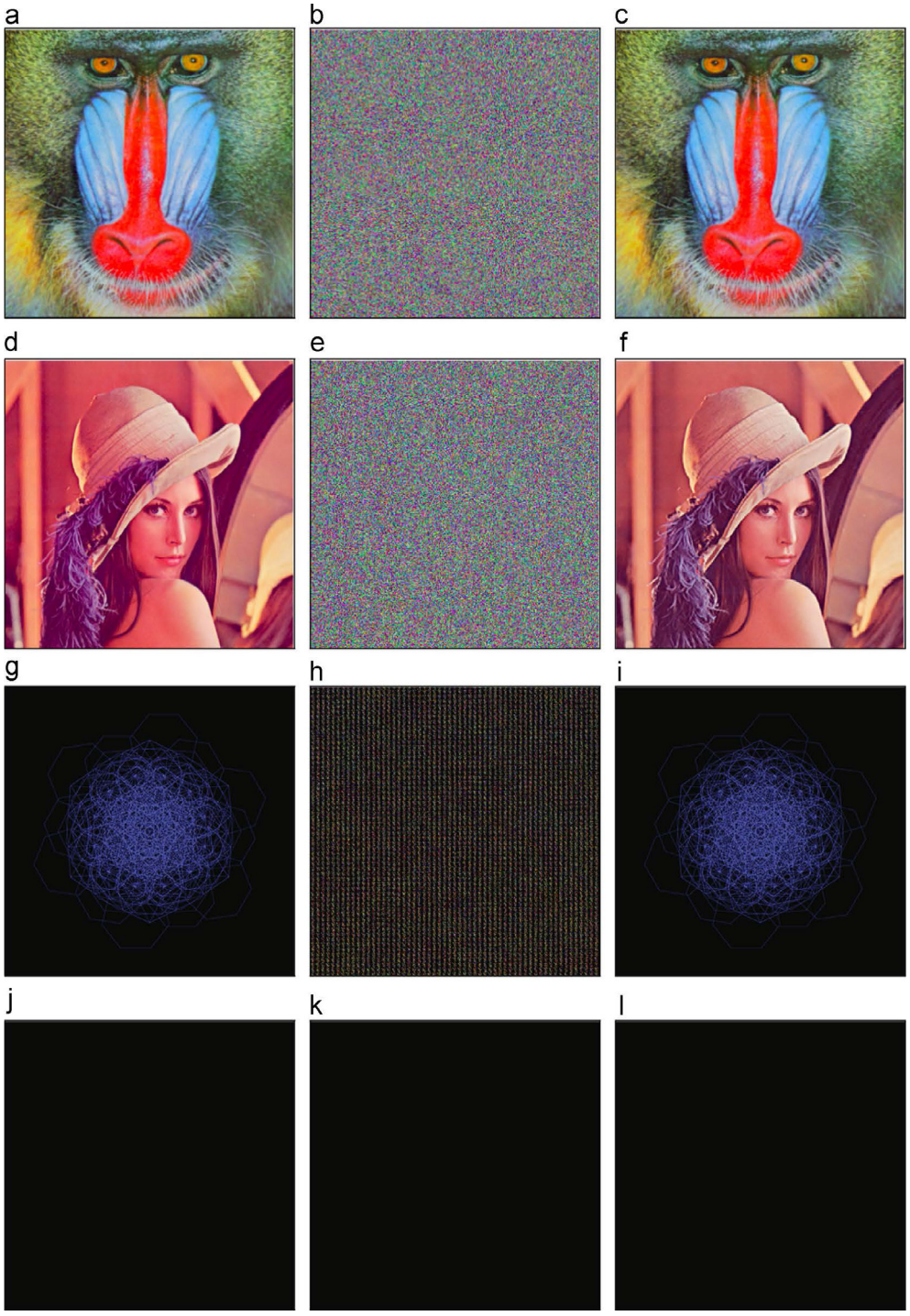


**Fig. 5.** "Simulations. (a) Original Baboon image. (b) Encrypted Baboon image. (c) Decrypted Baboon image. (d) Original Lena image. (e) Encrypted Lena image. (f) Decrypted Lena image. (g) Original hexfractal (sparse) image. (h) Encrypted hexfractal (sparse) image. (i) Decrypted hexfractal (sparse) image. (j) Original black image. (k) Encrypted black image. (l) Decrypted black image." (Provided in [24].)

to the keys. The recovery success rate for images of size $256 \times 256$ is almost 100%. For larger images, respectively more number of chosen plain images and approximation is required. For instance, Fig. 8 (with size of $512 \times 512$) is recovered using only two chosen plain images from cipher image and mean of absolute difference for the missing pixels. The simulation results demonstrate that the full visible pattern of the image is recovered by using only two chosen plain images and finding the mean value between the missing pixel values and the recovery rate is about 70%. In order to achieve a recovery rate close to 100%, for an image with size of $512 \times 512$ has to be cryptanalyzed using three to four chosen plain images. Nevertheless, the achieved results for this size with only two chosen plain images is considerable.

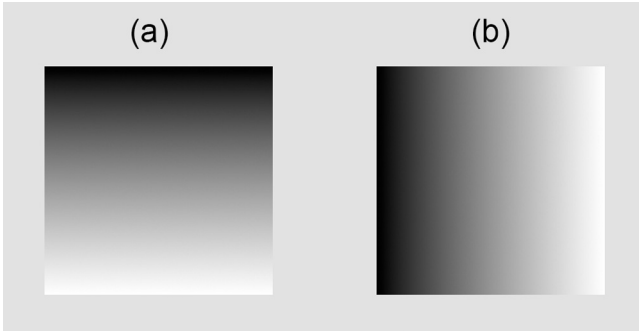


**Fig. 6.** Chosen plain-image.

## 4. Improvement

In order to improve the security of the image encryption algorithm, it should be modified such that the with minimum change of the plain image or the keys lead to a completely different cipher image. There exist numerous ways to achieve this goal and prevent the attacker from recovering the plain image. For instance, one method is by preventing the attacker from obtaining the substitution matrix [28]. Another method to secure the image encryption against chosen plaintext attack is by using a secondary diffusion method based on a cryptographically random source such as a properly modified chaotic map [29] before and after the confusion step. In order to apply this improvement initially the plain image should be encrypted using a chaotic map with having one of the control parameters depend on the previously ciphered plain pixel. In the second step the shuffling method proposed by the image encryption algorithm under study should be applied. In the last round, the shuffled image pixels need to be diffused using the same strategy applied in the initial step but in reverse direction. This method can guarantee successful diffusion and confusion of the ciphered image, and the attacker may not be able to retrieve the substitution matrix.

## 5. Conclusion

In this study, the security of a "A new RGB image encryption algorithm based on DNA encoding and elliptic curve DiffieHellman cryptography" is evaluated. From the simulation results it is found that the proposed algorithm in [24] is a shuffling only image encryption algorithm, and lacks the confusion and diffusion characteristics required for a secure image encryption algorithm. In addition, in this paper a new straightforward cryptanalysis method, similar to the reverse permutation map method used in [6,25,27] is proposed. The proposed method is capable of recovering any ciphered image by the same keys with access to only two


**Fig. 7.** (a) Sample image $P_{256\times256}$, (b) encrypted, (c) recovered by $V$ and $H$ generated only 2 chosen plain images (see Fig. 6).

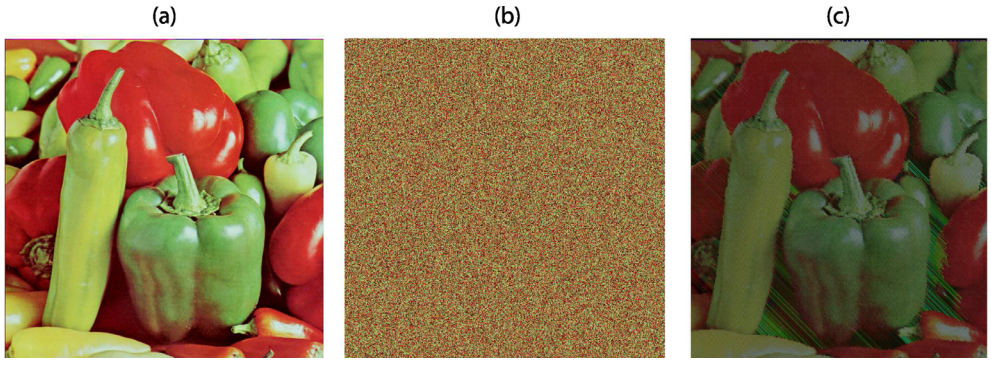


**Fig. 8.** (a) Sample image $P_{512\times512}$, (b) encrypted red, green and blue layers, (c) recovered by $V$ and $H$ generated only 2 chosen plain images (see Fig. 6). (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

chosen plain images. In conclusion, it can be stated that the image encryption algorithm [24] is not recommended in applications requiring a high level of security.

## Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the. This research is supported by School of Computer Sciences, Universiti Sains Malaysia.

## References

[1] S. El Assad, M. Farajallah, A new chaos-based image encryption system, Signal Process.: Image Commun. 41 (2015) 144–157, http://dx.doi.org/10.1016/j.image.2015.10.004.
[2] A.A.A. El-latif, L. Li, N. Wang, Q. Han, X. Niu, A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces, Signal Process. 93 (11) (2013) 2986–3000, http://dx.doi.org/10.1016/j.sigpro.2013.03.031.
[3] M. François, T. Grosges, D. Barchiesi, R. Erra, A new image encryption scheme based on a chaotic function, Signal Process.: Image Commun. 27 (3) (2012) 249–259, http://dx.doi.org/10.1016/j.image.2011.11.003.
[4] X. Li, C. Li, I.-K. Lee, Chaotic image encryption using pseudo-random masks and pixel mapping, Signal Process. (2015) 1–16, http://dx.doi.org/10.1016/j.sigpro.2015.11.017.
[5] S. Mohammad Seyedzadeh, S. Mirzakuchaki, A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, Signal Process. 92 (5) (2012) 1202–1215, http://dx.doi.org/10.1016/j.sigpro.2011.11.004.
[6] S. Li, C. Li, G. Chen, N.G. Bourbakis, K.-T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Process.: Image Commun. 23 (3) (2008) 212–223, http://dx.doi.org/10.1016/j.image.2008.01.003.
[7] A. Kadir, A. Hamdulla, W.-Q. Guo, Color image encryption using skew tent map and hyper chaotic system of 6th-order cnn, Optik – Int. J. Light Electron Opt. 125 (5) (2014) 1671–1675, http://dx.doi.org/10.1016/j.ijleo.2013.09.040.
[8] I.S. Sam, P. Devaraj, R.S. Bhuvaneswaran, I.S.S.P. Devaraj, R.S. Bhuvaneswaran, A novel image cipher based on mixed transformed logistic maps, Multimedia Tools Appl. 56 (2) (2010) 315–330, http://dx.doi.org/10.1007/s11042-010-0652-6.
[9] Z. Hua, Y. Zhou, C.-M. Pun, C.P. Chen, 2d sine logistic modulation map for image encryption, Inform. Sci. 297 (2015) 80–94, http://dx.doi.org/10.1016/j.ins.2014.11.018.
[10] Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on 3D chaotic baker maps, Int. J. Bifurcat. Chaos 14 (10) (2004) 3613–3624, http://dx.doi.org/10.1142/S021812740401151X.
[11] C. Dong, Color image encryption using one-time keys and coupled chaotic systems, Signal Process.: Image Commun. 29 (5) (2014) 628–640, http://dx.doi.org/10.1016/j.image.2013.09.006.
[12] A. Akhshani, A. Akhavan, S.-C. Lim, Z. Hassan, An image encryption scheme based on quantum logistic map, Commun. Nonlinear Sci. Numer. Simul. 17 (12) (2012) 4653–4661, http://dx.doi.org/10.1016/j.cnsns.2012.05.033.
[13] S. Behnia, A. Akhavan, A. Akhshani, A. Samsudin, Image encryption based on the jacobian elliptic maps, J. Syst. Softw. 86 (9) (2013) 2429–2438, http://dx.doi.org/10.1016/j.jss.2013.04.088.
[14] A. Akhavan, H. Mahmodi, A. Akhshani, Proceedings of the 21th International Symposium on Computer and Information Sciences – ISCIS 2006, Istanbul, Turkey, November 1–3, 2006, Springer, Berlin, Heidelberg, 2006, pp. 963–971, Chapter: A New Image Encryption Algorithm Based on One-Dimensional Polynomial Chaotic Maps.
[15] R. Boriga, A.C. Dascalescu, I. Priescu, A new hyperchaotic map and its application in an image encryption scheme, Signal Process.: Image Commun. 29 (8) (2014) 887–901, http://dx.doi.org/10.1016/j.image.2014.04.001.
[16] S. Fu Yan, L. Shu Tang, L. Zong Wang, Image encryption using high-dimension chaotic system, Chinese Phys. 16 (12) (2007) 3616–3623, http://dx.doi.org/10.1088/1009-1963/16/12/011.
[17] L. Liu, Q. Zhang, X. Wei, A RGB image encryption algorithm based on DNA encoding and chaos map, Comput. Electr. Eng. 38 (5) (2012) 1240–1248, special issue on Recent Advances in Security and Privacy in Distributed Communications and Image processing.
[18] H. Liu, X. Wang, A. Kadir, Image encryption using DNA complementary rule and chaotic maps, Appl. Soft Comput. 12 (5) (2012) 1457–1466, http://dx.doi.org/10.1016/j.asoc.2012.01.016.
[19] Y.-Q. Zhang, X.-Y. Wang, J. Liu, Z.-L. Chi, An image encryption scheme based on the MLNCML system using DNA sequences, Opt. Lasers Eng. 82 (2016) 95–103, http://dx.doi.org/10.1016/j.optlaseng.2016.02.002.
[20] X. Wu, H. Kan, J. Kurths, A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps, Appl. Soft Comput. 37 (2015) 24–39, http://dx.doi.org/10.1016/j.asoc.2015.08.008.
[21] X. Li, L. Wang, Y. Yan, P. Liu, An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems, Optik – Int. J. Light Electron Opt. 127 (5) (2016) 2558–2565, http://dx.doi.org/10.1016/j.ijleo.2015.11.221.
[22] T. Xie, Y. Liu, J. Tang, Breaking a novel image fusion encryption algorithm based on {DNA} sequence operation and hyper-chaotic system, Optik – Int. J. Light Electron Opt. 125 (24) (2014) 7166–7169, http://dx.doi.org/10.1016/j.ijleo.2014.07.111.
[23] Y. Liu, J. Tang, T. Xie, Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map, Opt. Laser Technol. 60 (5) (2014) 111–115, http://dx.doi.org/10.1016/j.optlastec.2014.01.015, arXiv:1307.4279.
[24] M. Kumar, A. Iqbal, P. Kumar, A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography, Signal Process. 125 (2016) 187–202, http://dx.doi.org/10.1016/j.sigpro.2016.01.017.
[25] F.-G. Jeng, W.-L. Huang, T.-H. Chen, Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes, Signal Process.: Image Commun. 34 (2015) 45–51, http://dx.doi.org/10.1016/j.image.2015.03.003.
[26] C. Li, Cracking a hierarchical chaotic image encryption algorithm based on permutation, Signal Process. 118 (2016) 203–210, http://dx.doi.org/10.1016/j.sigpro.2015.07.008.
[27] A. Akhavan, A. Samsudin, A. Akhshani, Cryptanalysis of an improvement over an image encryption method based on total shuffling, Opt. Commun. 350 (2015) 77–82, http://dx.doi.org/10.1016/j.optcom.2015.03.079.
[28] M. Li, S. Liu, L. Niu, H. Liu, Cryptanalyzing a chaotic encryption algorithm for highly autocorrelated data, Opt. Laser Technol. 86 (2016) 33–38, http://dx.doi.org/10.1016/j.optlastec.2016.06.012.
[29] A. Akhavan, A. Samsudin, A. Akhshani, A symmetric image encryption scheme based on combination of nonlinear chaotic maps, J. Franklin Inst. 348 (8) (2011) 1797–1813, http://dx.doi.org/10.1016/j.jfranklin.2011.05.001.