Performance Evaluation of AES, ECC and Logistic Chaotic Map Algorithms in Image Encryption

https://doi.org/10.3991/ijim.v17i10.38787

Farah Tawfiq Abdul Hussien(✉), Teaba Wala Aldeen Khairi
Computer Science Department, University of Technology-Iraq, Baghdad, Iraq
Farah.T.Alhilo@uotechnology.edu.iq

Abstract—In these days of technology, the usage of images has become increasingly high especially now that almost **e**veryone has access to internet. Also, image helps us to learn, grabs our attention, explains complicated concepts as well as inspires us. Sharing these images is essential and therefore image encryption algorithms are proposed to secure the transmission of these image from many types of attacks such as Man-in-the-middle attack (MITM). In this paper, we proposed a hybrid security system that consist of Elliptic Curve Cryptography (ECC) and Advanced Encryption System (AES). Where ECC is used to generate private/public keys and AES is for encryption and decryption of the image using the ECC generated keys. The system works as follows; it begins by inserting the image to be encrypted which is "lena.png" of size 256*256 and passing it to AES Algorithm along with the generated public key. Then, in AES algorithm, the public key is hashed then used to encrypt the image with AES encryption algorithm. On the other hand, the decryption algorithm works as follows; inserting the encrypted image then calculating the decryption key to use it to decrypt the image using AES decryption algorithm. Finally, our experimental results shows that the National Institute of Standards and Technology (NIST) test shows that the ECC generated keys have better randomness than using only AES generated keys. Also, the encrypted image histogram show that the image pixels values are well distributed across all three channels R, G and B. This shows that the hybrid system is a step further to get a more secure image encryption system against attacks with the generated ECC keys. To get further, Logistic chaotic map has been used to encrypt images for comparison purposes with AES and ECC generated images in terms of randomness, security and histogram.

Keywords—Man-in-the-middle attack (MITM), Elliptic Curve Cryptography (ECC), Advanced Encryption System (AES), National Institute of Standards and Technology (NIST)

1 Introduction

Images have become an essential part of daily lives. Sharing images gives us a joyful experience and it's done very easily especially with the advanced technology that's used to provide us with Internet. Even though there's so much entertainment we got out of images, Internet is simply consisting of interconnected networks which is not secure. Images could be confidential such as medical and militant images which must be accessed only by authorized users [7]. Here, cryptography plays it's secured these images

to be reached only by authorized users. Different methods of cryptography are proposed for the purpose of image encryption using symmetric methods, asymmetric methods and the mix between them (hybrid). Hybrid ECC (Elliptic Curve Cryptography) and AES (Advanced Encryption System) is proposed, in which ECC is for the purpose of generating private-public keys while AES is for the encryption and decryption of the image using the ECC keys. In this paper, ECC is used which a modern substitute of RSA algorithm that gives a very high-speed signatures, key agreement and key generation than RSA due to its smaller keys and signatures [8]. The previously mentioned propertied show that ECC is a one of the best choices in contrast to others. This cryptosystem uses a discrete logarithm problem (DLP) the takes an elliptic curve chose point. All of the makes it become the top choice for mobile communication [9]. On the other hand, AES uses the generated key to encrypt the data with a private key and later decrypt the data with the public key. Cryptosystem algorithms are sub exponentially difficult or linearly difficult [10].

2 Related work

Toughi Shahriyara, Mohammad H. Fathia and Yoones A. Sekhavatb, 2017, [1], in their paper proved that a clear example of effective cryptography is Elliptic curve cryptography (ECC). It has a very efficient key size in contrast to other algorithms public key. The phase of generating random depends on a changing point (G) that is a generator of a curve to obtain random sequences. Furthermore, AES that is applied for encrypting image using the sequences acquires an arbitrary key. The usage of AES with a well distributed random numbers provides a prominent method of encryption. Their experimental results showed that their proposed system satisfies the cryptography basics that includes correctness and simpleness. Furthermore, their evaluation results showed that their proposed method is both secure and effective. Chiranji Lal Chowdhary, Pushpam Virenbhai Patel, Krupal Jaysukhbhai Kathrotia, Muhammad Attique, Kumaresan Perumal and Muhammad Fazal Ijaz, 2020, [2], in their paper, mentioned that most of imaging methods and techniques used to encrypt any digital media are either symmetric or asymmetric encryption algorithms. The majority of research works of encryption and decryption mainly uses Advanced Encryption Standard (AES) algorithm. The proposed system of their paper is performance analysis for image encryption and decryption using hybridization of Elliptic Curve Cryptography (ECC) alongside Hill Cipher (HC), while on the other hand, ECC with Advanced Encryption Standard (AES) with ElGamal alongside the Double Playfair Cipher (DPC). The basis of this analysis are the following parameters: (a) Time of Encryption and decryption, (b) Encrypted image entropy, (c) The decrypted image intensity loss, (d) Peak Signal to Noise Ratio (PSNR), (e) No. of Pixels Change Rate (NPCR), and (f) Unified Average Changing Intensity (UACI). The ease of implementation and speed of symmetric algorithms, along with the asymmetric algorithms improved security are both involved within the hybrid process. ECC and ElGamal uses asymmetric key cryptography, on the other hand, HC, AES, and DPC use symmetric key algorithms. ECC with AES are the best for private or remote communications alongside image of smaller sizes based on the

encryption and decryption time. Test cases along with metric measurement showed that ECC and HC have a very well image encryption solution. Amal Hafsa and Anissa Sghaier, 2020, [3], in their paper, talked about the internet requirement for wireless communication in this era which is rising progressively, therefore, securing communication on unsecure wireless channels is required. The results showed that the analysis is based on various parameters which include correlation, avalanche effect, decryption time, encryption time and storage. Samiksha Sharma and Vinay Chopra, 2016, [4], in their paper, they defined encryption as a very commonly known method applied over data and text and now images also. We have focused over image encryption mainly in our work. Elliptical curve cryptography (ECC) is classic and conventional approach has been applicable for image encryption and cryptography. The process of ECC is based on key generation technique and has been provided comparative results to RSA algorithm. ROI proposed over the existing approach will reduce the complexity as it discards the unused domain in image which is not needed to be encrypted. Amod Kumar Sahwal, Brij Kishore, Pramod Singh Rathore and Jyotir Moy Chatterjee, 2018, [5], in their paper, explained that in the advances of communication and technology have a major impact on the security levels required to secure digital media transmission. In their paper, they proposed a medical encryption security method that has the form of images. Their proposed method Encryption scheme is applied using modified Identity Based. Elliptic Curve Cryptography (ECC) is the encryption algorithm used in order to generate key pairs while the Advanced Encryption Standard (AES) is used to generate symmetric keys as well as encrypt process. Histogram analysis, computation time and statistical analysis are the bases of testing of the proposed method. The outcome of these tests' techniques showed that the proposed system was of high resistant against statistical attacks even though that its computing time is slow. Their proposed system has a higher entropy and is capable of making pixels in the cipher image distributed evenly compared to other methods.

Dian Neipa Purnamasari, Amang Sudarsono and Prima Kristalina, 2019, [6], in their paper, mentioned that the complexity of computing in an asymmetric cryptography makes it slow, while the symmetric ones is fast. The latter suffers from a major gap that is the security level of key exchange. To fix this issue, an efficient AES-ECC hybrid cryptosystem is proposed which has the advantages of the advanced encryption standard (AES) that speeds the data encryption up and on the other hand, the asymmetric elliptic curve cryptography (ECC) is used to secure the interchange of symmetric key session. they proposed an enhanced ECC hardware architecture that relies on L´opez-Dahab scalar multiplication (on Cyclone IV.E).

3 Symmetric and asymmetric encryption

As mentioned earlier, there are many different methods for encryption purposes, the symmetric, asymmetric and the hybrid ones [11]. Symmetric encryption methods use only one key for encryption as well as decryption [12]. A single key usage for encryption and decryption a straightforward operation and that's why it's knows as "symmetric" [13]. Symmetric method is considered a great technique is the simplicity of its

process where it lies in a single key usage for encryption and decryption [14]. The results shows that symmetric methods:

- Are remarkably faster than its opponent (asymmetric encryption)
- Less computational power
- Do not dampen internet speed.

From above, a conclusion is made that in case of large amount of data, symmetric encryption proves to be a great one to pick [15]. Symmetric encryption methods use multiple keys for both encryption and decryption operations [16]. Two mathematically connected to one another encryption keys are used. One of the keys is called “public key”, while the other is known as “private key” [17]. Asymmetric encryption method is also called “public key cryptography”. Asymmetric method is a great technique for many reasons [18].

- The Advantage of using asymmetric encryption is the security it offers. Where, the public key is for encrypting the data, while private key is for decryption, which needs to be saved in a safe place. This process makes sure that the data stays safe from man-in-the-middle attacks. Another thing to be pointed out is that the need to meet offline for keys exchanging is eliminated with the help of public key that allowed the process of on structing an encrypted connection.
- Another crucial advantage of asymmetric method is that is provides authentication. The data is encrypted using public key is used only for the purpose of decrypting using the private key associated with it. As a result, it ensures that the data is only accessed as well as decrypted using the designated recipient.

4 Hybrid approach

Hybrid approach is a combination of symmetric and asymmetric encryption is proposed [19]. To begin with, let’s make clear that the name we call “hybrid encryption" is not a “method” such as symmetric or asymmetric encryptions but it takes the best out of both operations to construct a powerful encryption system [20]. Both main encryption methods (symmetric and asymmetric) have their own downsides and disadvantages. Symmetric encryption is the best large amount of data for a high-speed encryption, but it doesn’t support identity verification [21]. While, asymmetric encryption ensures that data is accessed by the intended recipient. The verification process tends to make the encryption operation very slow especially if it implemented at large scale of data [22-25]. In applications that applies a series of back-and-forth communications between sender and the recipient, hybrid encryption is the one to use. This way, the identity of sender and recipient is verified with the help of private-public key pair. When both sides have authenticated their own identities, data encryption starts through symmetric encryption which uses the session key. This makes sures that the transmission is fast for a large amount of data that are sent and received over the internet [26].

5 Proposed system

The Proposed system is a system composed of two main algorithms: Elliptic Curve Cryptography (ECC) along with Advanced Encryption Standard (AES). Where ECC is for generating a private-public key pair. While the algorithm used for encryption and decryption operations using the keys generated in ECC.

5.1 Proposed system steps

The proposed system works as follows:

1. Reading the image to be encrypted (cameraman or lena) then resizing the image to 256*256.
2. Generation ECC private-public key pair assuming that we use a cryptographic elliptic curve for a finite field, alongside its generator point G. To calculate an encryption and decryption shared secret key, it is as follows:
   (a) Generating Private Key which is an integer that is typically integers of 256-bit.
   (b) Calculating Public Key (Public Key = Private Key * curve point) which is ECC point - pairs (x, y) coordinates that are integers and lies on the curve. Because of this coordinates properties, elliptic curve points are easily compressed to result only a single coordinate + 1 bit (that one bit can be even or odd). Therefore, this compressed public key, associated to a 256-bit elliptic curve private key that is an integer of 257-bit.
3. ECC Encryption process of starts by:
   (a) Passing image and Public Key to ECC Encryption Algorithm.
   (b) Generating Ciphertext Private Key = new random private key.
   (c) Calculate the ECDH shared secret (Shared ECC Key = Ciphertext Private Key * Public Key).
   (d) Calculating Secret Key (which is calculated by hash then digest operations on Shared ECC Key which is generated in ECC Encryption Algorithm).
   (e) Calculating Ciphertext Public Key = Ciphertext Private Key * G.
   (f) Passing the image to be encrypted plus the Secret Key to AES Encryption Algorithm.
   (g) Returning both the Private Key (used for symmetric encryption) and the randomly generated Ciphertext Public Key (in order to calculate the decryption key).
   (h) See the flowchart below in Figure 1.\

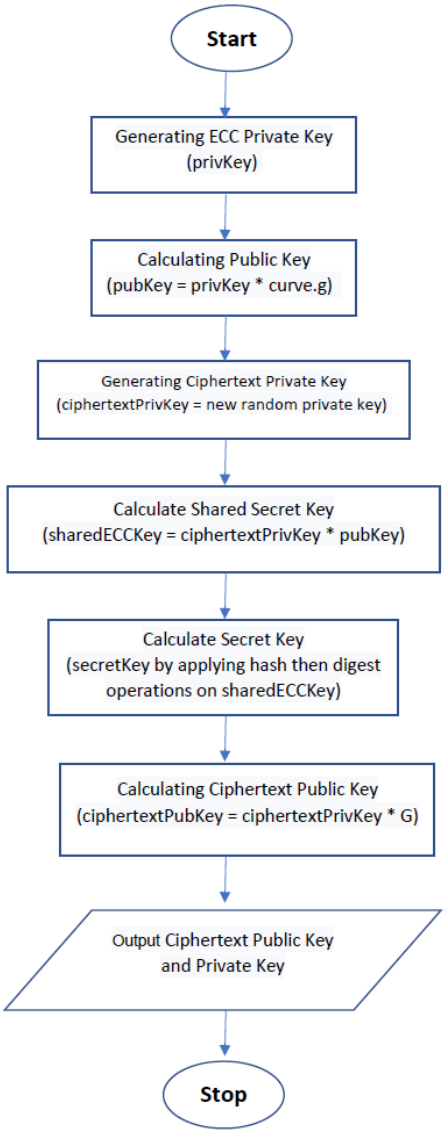


Fig. 1. ECC Encryption Flowchart

4. AES Encryption process starts as follows:
   (a) Passing the image to be encrypted plus the Secret Key to AES Encryption.
   (b) Encoding the Secret Key with Hash Library
   (c) Calculating new AES Cipher Key with the encoded Secret Key using AES CFB Mode
   (d) Encrypting the image with the ciphered key.
   (e) Saving the encrypted image. See the flowchart below in Figure 2

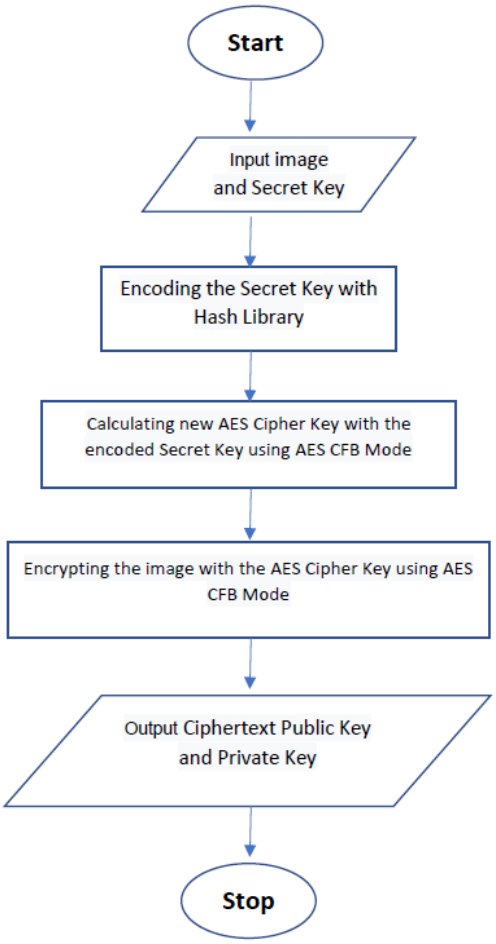


Fig. 2. AES Encryption Flowchart

5. ECC Decryption process of starts by:
   (a) Passing the encrypted image (from the AES Algorithm), Private Key and Ciphertext Public Key (that's returned from the ECC Encryption Algorithm) to ECC Decryption Algorithm.
   (b) Calculating Decryption Key (Private Key, Ciphertext Public Key) which is Shared ECC Key (Shared ECC Key = Private Key * Ciphertext Public Key).
   (c) Calculating Secret Key (which is calculated by hash then digest operations on Shared ECC Key).
   (d) Passing image and Secret Key and Encrypted Image to AES Decryption Algorithm.
   (e) See the flowchart below in Figure 3

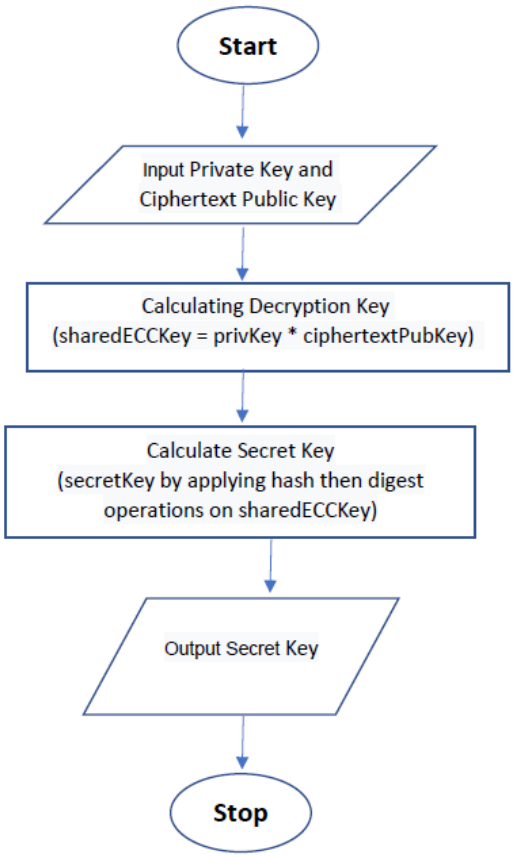


Fig. 3. ECC Decryption Flowchart

6. AES Decryption process starts as follows:
   (a) Passing the image to be encrypted plus the Secret Key to AES Decryption.
   (b) Encoding the Secret Key with Hash Library
   (c) Calculating AES Decipher Key with the encoded Secret Key using AES CFB Mode
   (d) Decrypting the image with the decipher key.
   (e) Saving the Decrypted image.
   (f) See the flowchart below in Figure 4

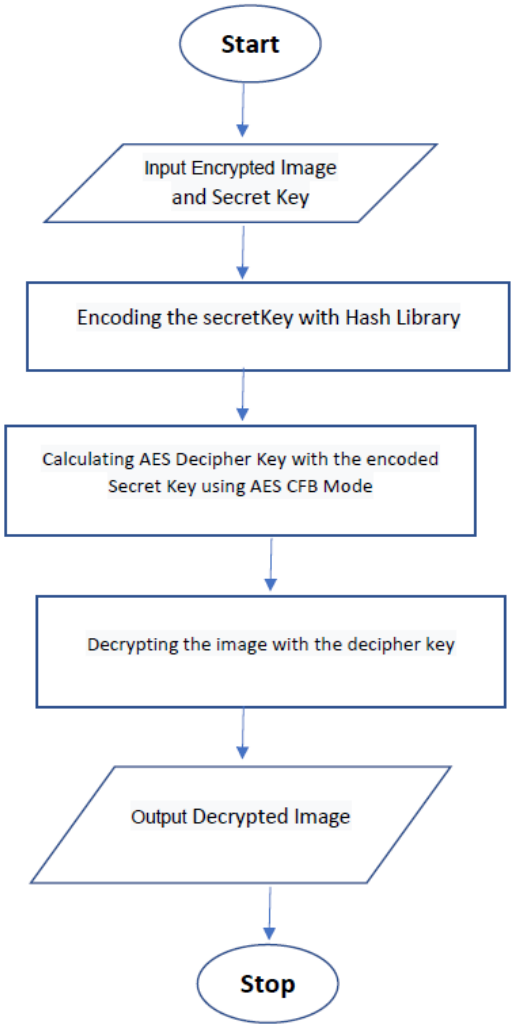


Fig. 4. AES Decryption Flowchart

7. Logistic Map Encryption process starts as follows:
   (a) Generate Key for logistic sequence generator
   (b) Insert Image
   (c) Permutate image array with the generated key from Sequence Generator
   (d) Diffuse the permutate image array
   (e) Transpose the image
   (f) Repeat step c to e to encrypt the entire image
   (g) Output a ciphered image. See the flowchart in Figure 5

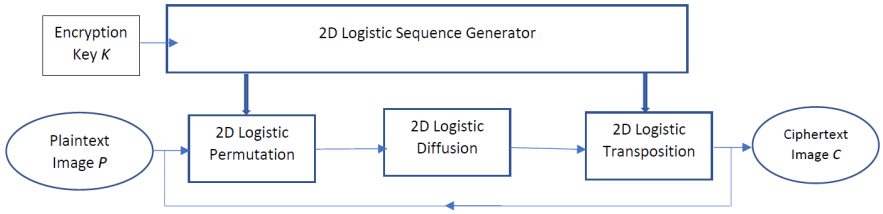


Fig. 5. Logistic Map Encryption Flowchart

8. Logistic Map Decryption process starts as follows:
   (a) Insert the encryption key for logistic sequence generator
   (b) Insert the encrypted image
   (c) Transpose the encrypted image
   (d) Diffuse the result of transposed encrypted image array
   (e) Permutate the result into it's original form
   (f) Repeat step c to e to decrypt the entire image
   (g) Output original image. See the flowchart in Figure 6

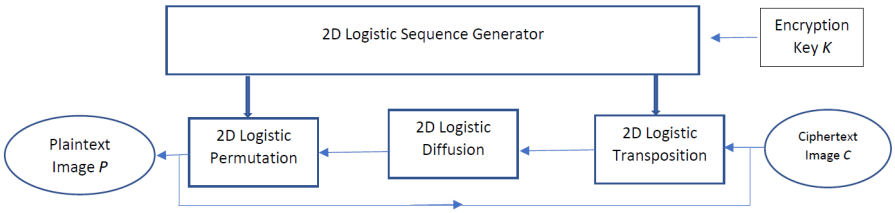


Fig. 6. Logistic Map Encryption Flowchart

5.2 Proposed system algorithm

The proposed system algorithm is shown below:

```
Algorithm: Proposed System Algorithm
Input: Image to be encrypted
Output: Decrypted Image
Begin:
Step 1: Starting ECC Encryption Algorithm
  Step 1.1: Generate Private Key = Randomly Generated
Key typically 256-bit integers
  Step 1.2: Calculate Public Key = Private Key * EC
Point
  Step 1.3: Generating Ciphertext Private Key = new
random Private Key.
  Step 1.4: Calculate Shared ECC Key = Ciphertext Pri-
vate Key * Public Key
```

Step 1.5: Calculating Secret Key = Generating ECC Point to 256 Bit Key by Digest and Hash operations on Shared ECC Key.

Step 1.6: Calculating Ciphertext Public Key = Ciphertext Private Key * EC Point

Step 2: Starting AES Encryption Algorithm

Step 2.1: Encoding the Secret Key with Hash Library.

Step 2.2: Generating new AES Cipher Key with the encoded Secret Key using AES CFB Mode.

Step 2.3: Encrypting the image with the AES Cipher Key using AES CFB Mode.

Step 3: Starting ECC Decryption Algorithm

Step 3.1: Calculating Shared ECC Key = Private Key * Ciphertext Public Key

Step 3.2: Calculating Secret Key = Generating EC Point to 256 Bit Key by Digest and Hash operations on Shared ECC Key.

Step 4: Starting AES Decryption Algorithm

Step 4.1: Encoding the Secret Key with Hash Library.

Step 4.2: Generating AES Decipher Key with the encoded Secret Key using AES CFB Mode.

Step 4.3: Decrypting the image with the AES Decipher Key using AES CFB Mode.

End

Algorithm: Logistic Map Algorithm
Input: Image to be encrypted
Output: Decrypted Image
Begin:
Step 1: Starting Logistic Map Encryption Algorithm

Step1.1: Generate Key for logistic sequence generator

Step1.2: Insert Image

Step1.3: Permutate image array with the generated key from Sequence Generator

Step1.4: Diffuse the permutate image array

Step1.5: Transpose the image

Step1.6: Repeat step b to e to encrypt the entire image

Step1.7: Output a ciphered image

Step 2: Starting Logistic Map Decryption Algorithm

Step2.1: Insert the encryption key for logistic sequence generator

Step2.2: Insert the encrypted image

Step2.3: Transpose the encrypted image

```
    Step2.4: Diffuse the result of transposed encrypted
image array
    Step2.5: Permutate the result into it's original form
    Step2.6: Repeat step 2.3 to 2.5 to decrypt the entire
image
    Step2.7: Output original image
  End
```

6 Experimental results and discussion

6.1 Randomness test results

For the purpose of calculating the casualness of the key generated using the proposed system, The National Institute of Standards and Technology (NIST) statistical tests are used for the generated key. These tests include 15 tests, such as monobit test, frequency, Serial test, cumulative sums, approximate entropy test, runs and others. The stream of bits for the generated key is thought-out of being a random in case of the P-value of each test is equal or greater than 0.01, where P-value is considered the distribution of the resulted value which is extracted out from each test plus 0.01 value of threshold that is used to tell whether or not the stream of bits are random. The better randomness occurs when of the P-value approaches to one, on the other hand, determinant sequence is in case of zero P-value. These tests for ECC and AES are presented in Table 1. Figure 7 shows a chart of the table data to get a visualization point of view of how using ECC key has a better randomness that others.

Table 1. NIST SP800_22 for testing the randomness of key

Number	P-Value of Randomness Tests/Test name	AES	ECC	Logistic Map
1	random_excursion_variant_test	0.220375531907715	0.0017762968464917	0.00114384573708036
2	cumulative_sums_test	0.906386327991525	0.573147563111154	0.124895427063915
3	approximate_entropy_test	0.0290568095703588	0.88491804105452	1.59201186447293E-14
4	serial_test	0.0817654162447216	0.821091879049193	2.15431360727174E-11
5	maurers_universal_test	0.00196981608586774	0.997330475852347	0.34563002716143
6	longest_run_ones_in_a_block_test	0.120781936262129	0.75279409926277	1
7	runs_test	0.0174956965355434	0.86236055401572	0.752820658686577
8	frequency_within_block_test	0.934889686635758	0.925826198405844	0.730786486588766
9	monobit_test	0.900523550339774	0.381573905705021	0.0775561667436655

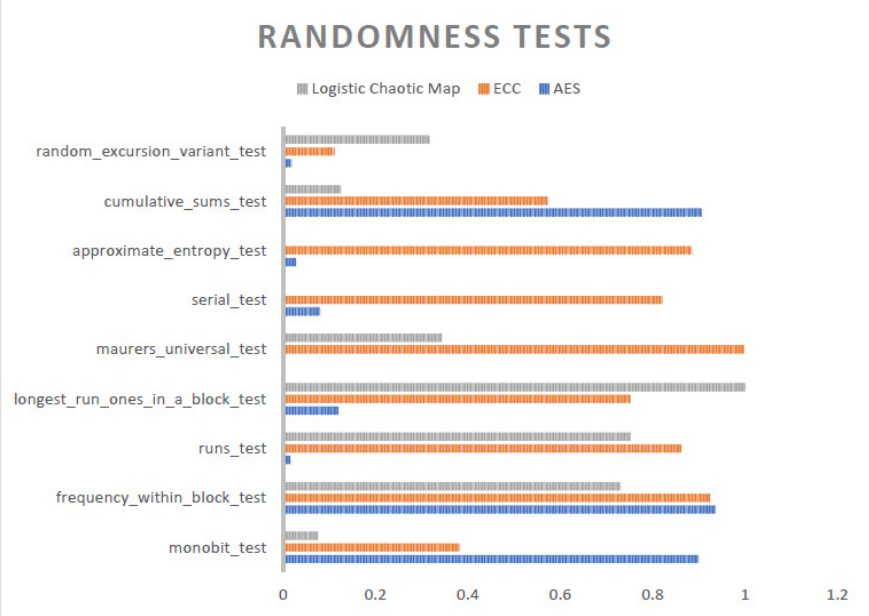


Fig. 7. Randomness Test Chart

6.2 Analysis of histogram

The histogram analysis of a ciphertext image is one of the top straight-forward methods for illustrating the quality of image encryption. An image encryption method is considered to be good when it encrypts a plaintext image into a for that is randomly incomprehensible. Therefore, a good image encryption method generates a uniformly distributed intensity histogram ciphered image. Histogram analysis denotes the delivery of each pixel value. The plain pixels distribution usually is uneven, also some pixels do have a unique incidence within image. Which makes it worth changing. The cipher image must be distributed in the proposed system to resist and attack on the ciphered image. Original image can be seen in Figure 7.1, lena.png, with a size of 256 to 256, Figure 7.2, shows the histogram of the image with RGB channels combined while 7.3, 7.4 and 7.5 are the original image R, G, and B channels histograms respectively. On the other hand, Figure 8.1 displays lena.png ciphered image using AES with ECC generated key and the other Figures 8.2, 8.3, 8.4 and 8.5 are the RGB channels combined, R, G and B channels respectively. While Figure 9 with it's parts follows the same above pattern for encrypting an image with Logistic Map.

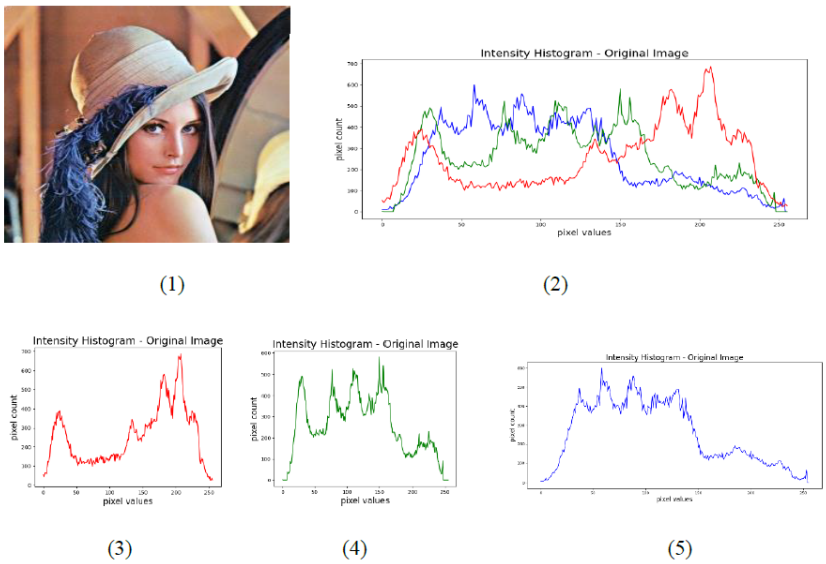


Fig. 8. lena.png original image. (1) Original image lena.png of size 256 x 256, (2) Original RGB channels combined (3) Original Red Channel Histogram, (4) Original Green Channel Histogram and (5) Original Blue Channel Histogram

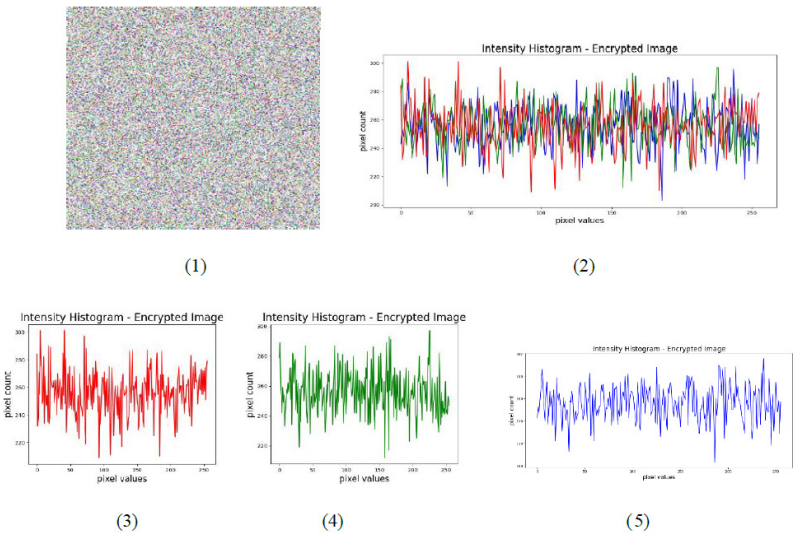


Fig. 9. lena.png ciphered image histogram Using ECC Keys. (1) Ciphered image lena.png of size 256 x 256, (2) RGB channels combined (3) R Channel, (4) G Channel and (5) B Channel

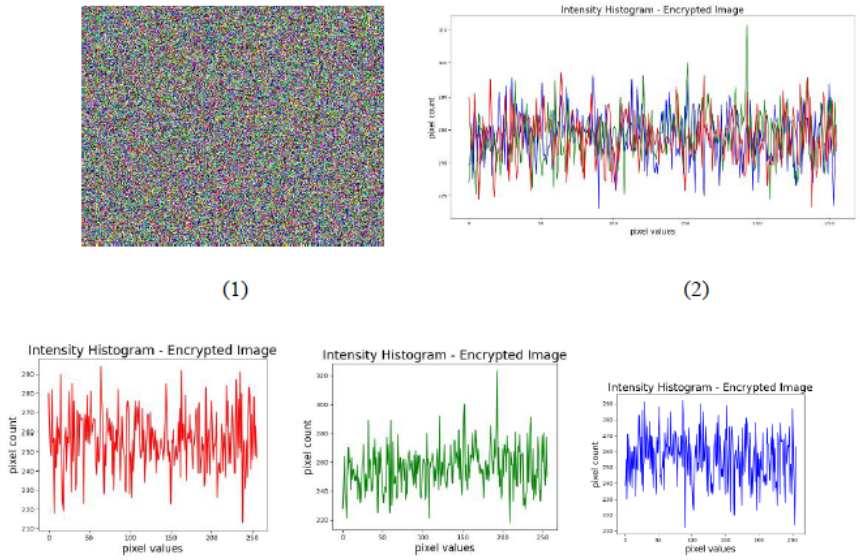


Fig. 10. lena.png ciphered image histogram Using Logistic Map Keys. (1) Ciphered image lena.png of size 256 x 256, (2) RGB channels combined (3) R Channel, (4) G Channel and (5) B Channel

6.3 Correlation coefficient analysis

The most encrypted image statistical analysis is the correlation coefficient analysis. In original image, testing the correlation between two pixels and encrypted images. And if algorithm of image encryption takes over the entire p image properties, then it's considered to be successful, and resulted image (encrypted) is fully randomized, also, highly uncorrelated. The two images are the said to be the same, unless the coefficient of similarity is equal to 1. In this situation, the encryption fails.

Table 2. Comparing correlation coefficient analysis for lena 256 × 256 ciphered with ECC generated key with ciphered with AES generated key

Channels	ECC Generated Key vs Default Key
Red	-0.005009706815386738
Green	-0.009605452396563073
Blue	0.005492132281781384

6.4 Adjacent pixel autocorrelation

Knowing that images have high redundancy, for this redundancy to be removed, it is recommended to use encryption algorithm. Therefore, the correlation between adjacent pixels in a direction (Horizontal) is calculated as a encryption performance metric.

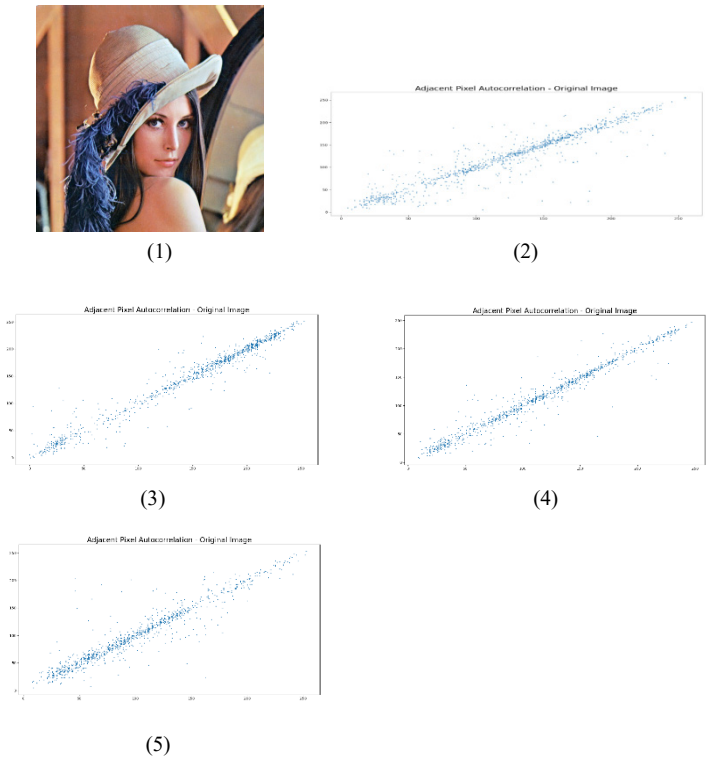


Fig. 11. Adjacent Pixel Autocorrelation of lena.png original image. (1) Original image lena.png of size 256 x 256, (2) Original RGB channels combined (3) Original Red Channel Histogram, (4) Original Green Channel Histogram and (5) Original Blue Channel Histogram

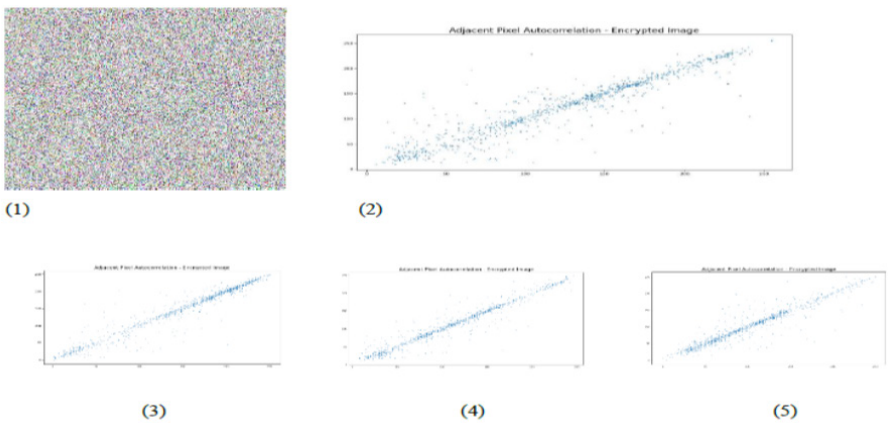
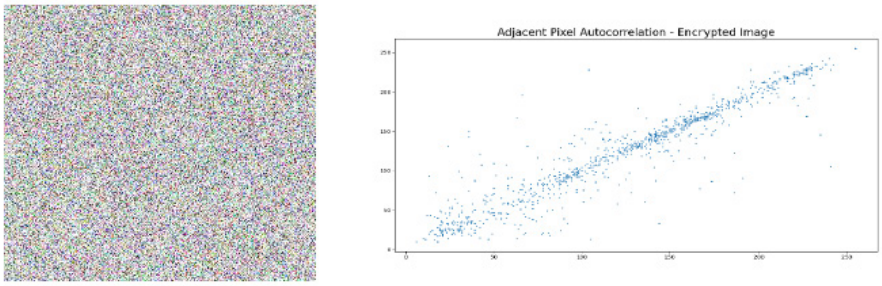


Fig. 12. Adjacent Pixel Autocorrelation of lena.png ciphered image histogram. (1) Ciphered image lena.png of size 256 x 256, (2) RGB channels combined (3) R Channel, (4) G Channel and (5) B Channel



(1) (2)

Fig. 13. Adjacent Pixel Autocorrelation of lena.png ciphered image histogram with Logistic Map. (1) Ciphered image lena.png of size 256 x 256, (2) RGB channels combined

6.5 Analysis of information entropy

Entropy review is another security factor of knowledge where ambiguity or randomness of images are characterized by it.

Table 3. Shannon Entropy

Channel	Ciphered with AES key	Ciphered with ECC key	Ciphered with Logistic Map
Red	7.997562962816608	7.996853454077184	7.997561072472019
Green	7.997431913267585	7.99721050226603	7.997445441557181
Blue	7.997061857446025	7.997198029890674	7.997359947004602

7 Conclusion

In this paper, Logistic chaotic map encryption has been used as well to compare it with AES-ECC encryption. Where ECC is used to generate private/public keys and AES is for encryption and decryption of the image using the ECC generated keys. The NIST suite tests shows that the p-value of the tests are closer to 1 for ECC key than the default AES key and the Logistic map as well, which tells that the randomness of the generated key from ECC algorithm is way better than all other generated keys. The reason behind using ECC it uses smaller keys and signatures than RSA itself. The experimental results of our paper showed our hybrid system is proved a very well randomization. Computation time for using ECC is higher than using AES symmetric encryption and logistic map too, computation time is a very well-accepted trade-off that can be accepted especially that it provides a very higher security level. For future work, new key generation technique of combining symmetric and asymmetric algorithms is still a way to go and of course computation time and other downside factor will be taking in our consideration.

8 References

[1] Mohanad, M. A. and Abdul Wahab, H. B., "Proposed New Blockchain Consensus Algorithm", International Journal of Interactive Mobile Technologies (iJIM), 16(20), pp. 162–176, 2022. https://doi.org/10.3991/ijim.v16i20.35549

[2] Abdulsattar, J. T., "Security Risks of the Metaverse World", International Journal of Iteactive Mobile Technologies (iJIM), 16(13), pp. 4–14, 2022. https://doi.org/10.3991/ijim.v16i13.33187

[3] Hafsa, A. and Sghaier, A., "An improved co-designed AES-ECC cryptosystem for secure data transmission", International Journal of Information and Computer Security. 13(1), pp 118-140, 2020. https://doi.org/10.1504/IJICS.2020.108145

[4] Sharma, S. and Chopra, V.," Analysis Of AES Encryption with ECC", Proceedings of International Interdisciplinary Conference on Engineering Science & Management, Held on 17th - 18th December 2016.

[5] Sahwal, A.K., Kishore, B., Rathore, P.S. and Chatterjee, J.M.,"An Advance proach of Looping Technique for Image Encryption Using In Commuted Concept Of ECC", International Journal of Recent Advances in Signal & Image Processing, vol 2(1), pp. 1-6,2018.

[6] Purnamasari, D.N., Amang Sudarsono,A. and Kristalina, ," Medical Image Encryption Using Modified Identity Based Encryption", EMITTER International Journal of Engineering Technology, ISSN: 2443-1168, pp. 524-536, 7(2) December 2019. https://doi.org/10.24003/emitter.v7i2.405

[7] H. T. ALRikabi and H. T. Hazim,"Enhanced Data Security of Communication System Using Combined Encryption and Steganography", International Journal of Interactive Mobile Technologies (iJIM), 15(16). https://doi.org/10.3991/ijim.v15i16.24557

[8] Gautam, Y., Gautam, B. P., & Sato, K.,"Experimental security analysis of SDN network by using packet sniffing and spoofing technique on POX and Ryu controller", International Conference on Networking and Network Applications (NaNA) (pp.394-399). IEEE, 7(2) December 2019. https://doi.org/10.1109/NaNA51271.2020.00073

[9] Gupta, K., Silakari, S., Gupta, R. And Khan, S.A., "An Ethical way for Image Encryption using ECC", First International Conference on Computational Intelligence, Communication Systems and Networks, 2009. https://doi.org/10.1109/CICSYN.2009.33

[10] Singh, L.D. and Singh, K. M.," Image Encryption using Elliptic Curve Cryptography. Procedia Computer Science", 54.pp. 472-481. https://doi.org/10.1016/j.procs.2015.06.054

[11] Abdul Hussien, F.T., Rahma, A.M.S. and Abdul Wahab, H.B.,"A Secure E-commerce Environment Using Multi-agent System", Intelligent Automation & Soft Computing Journal. 34(1). pp. 499-514, 2009. https://doi.org/10.32604/iasc.2022.025091

[12] Lozupone, V.," Analyze encryption and public key infrastructure (PKI)", International Journal of Information Management. 38(1). pp. 42-44. https://doi.org/10.1016/j.ijinfomgt.2017.08.004,2008

[13] Hassan, N.F., Ali, A.E., Wala Aldeen, T. and Ayad Al-Adhami, A.,"Video mosaic watermarking using plasma key", Indonesian Journal of Electrical Engineering and Computer Science. 22(2). pp. 11-20, 2009. https://doi.org/10.11591/ijeecs.v22.i2.pp619-628

[14] Khairi, T.W.A.," Framework For Modeling and Simulation of Secure Cloud Services", Iraqi Journal Of Computers, Communications, Control And Systems Engineering. 22(1) pp. 97-107, 2022. https://doi.org/10.33103/uot.ijccce.22.1.10

[15] Abdul Hussien, F.T., Rahma, A.M.S. and Abdul Wahab, H.B.," A Secure Environment Using A New Lightweight AES Encryption Algorithm For E-commerce Websites",Security and Communication Networks Journal. 2021. Article ID 9961172. pp. 1-15, 2022. https://doi.org/10.1155/2021/9961172

[16] Yassein, M.B., Aljawarneh,S. And Qawasmeh, E.," Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms", IEEE, International Conference on Engineering and Technology (ICET) , 2017. https://doi.org/10.1109/ICEngTechnol.2017.830–8215

[17] Hamada, A.S. and Farhan, A.K.,"Image encryption algorithm based on substitution principle and shuffling scheme", Engineering and Technology Journal. 38(3). pp. 98–103, 2020. https://doi.org/10.30684/etj.v38i3B.433

[18] Nanda, A., Nanda, P., He,X., Jamdagni, A. and Deepak Puthal.," A Hybrid Encryption Technique for Secure-GLOR: The Adaptive Secure Routing Protocol for Dynamic Wireless Mesh Networks", Future Generation Computer System Journal. 109. pp. 521-530, 2017. https://doi.org/10.1016/j.future.2018.05.065

[19] Ibraheem, M.N.F.," Proposed hybrid-encryption system for multicast network", Engineering and Technology Journal. 28(24). pp. 2027–2036,2021.

[20] Fangfang, W., Huazhong, W., Dongqing, C. and Yong, P.," Substation Communication security Research Based on Hybrid Encryption of DES and RSA", Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IEEE, 2013. https://doi.org/10.1109/IIH-MSP.2013.115

[21] Rahma, A.M.S., Abdul Hossen,A.M.J. and Dawood, O.A.," Public key cipher with signature based on diffie-hellman and the magic square problem", Engineering and Technology Journal. 34(1). pp. 1–15, 2016. https://doi.org/10.30684/etj.34.1B.1

[22] Liang, C., Ye, N. Malekian, R. and Wang, R.," The Hybrid Encryption Algorithm of Lightweight Data in Cloud Storage", 2nd International Symposium on Agent, Multi-Agent Systems and Robotics (ISAMSR),23-24 August 2016, Bangi, Malaysia. 10.1109/ISAMSR.2016.7810021. IEEE,2016.

[23] R. Mohamad, "Data hiding by using AES Algorithm: Data hiding by using AES Algorithm," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 4, pp. 112-119, 2022.

[24] Kh-Madhloom, "Dynamic Cryptography Integrated Secured Decentralized Applications with Blockchain Programming," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 2, pp. 21-33, 2022.

[25] H. T. Hazim, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," International Journal of Interactive Mobile Technologies, vol. 15, no. 16, pp. 144-157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[26] Abdul Hussien F.T., Rahma, A.M.S. and Abdul Wahab, H.B.," A Block Cipher Algorithm Based on Magic Square for Secure E-bank Systems" , Computers, Materials and Continua Journal. 34(1). pp. 1329–1346, 2016. http://dx.doi.org/10.32604/cmc.2022.027582

9 Authors

Farah Tawfiq Abdul Hussein Awarded her B.Sc., M.Sc. and Ph.D. degree from the University of Technology Baghdad Iraq in 2002, 2008 and 2022 respectively. Work as lecturer at the University of Technology - Department of Computer Sciences / Iraq – Baghdad.

Teaba Walaa Aldeen Khairi, B.Sc degree in computer science - software in 2005, M.Sc degree in 2015. Work as lecturer at the University of Technology - Department of Computer Sciences / Iraq – Baghdad.

Article submitted 2023-02-11. Resubmitted 2023-03-27. Final acceptance 2023-03-29. Final version published as submitted by the authors.