mathematics

MDPI

Article

Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher

Parveiz Nazir Lone [1], Deep Singh [1,2], Veronika Stoffová [3,4,*], Deep Chandra Mishra [5], Umar Hussain Mir [1] and Neerendra Kumar [6]

[1] Department of Mathematics, Central University of Jammu, Jammu 181143, India
[2] Department of Mathematics and Statistics, Central University of Punjab, Bathinda 151001, India
[3] Department of Mathematics and Computer Science, Trnava University, 91843 Trnava, Slovakia
[4] Department of Media and Educational Informatics, Faculty of Informatics, Eötvös Loránd University, 1053 Budapest, Hungary
[5] Department of Mathematics, Bhakt Darshan Govt. PG College, Jaiharikhal, Pauri Garhwal 246155, India
[6] Department of Computer Science and IT, Central University of Jammu, Jammu 181143, India
* Correspondence: nikastoffova@seznam.cz or veronika.stoffa@gmail.com

Abstract: In the present era of digital communication, secure data transfer is a challenging task in the case of open networks. Low-key-strength encryption techniques incur enormous security threats. Therefore, efficient cryptosystems are highly necessary for the fast and secure transmission of multimedia data. In this article, cryptanalysis is performed on an existing encryption scheme designed using elliptic curve cryptography (ECC) and a Hill cipher. The work shows that the scheme is vulnerable to brute force attacks and lacks both Shannon's primitive operations of cryptography and Kerckchoff's principle. To circumvent these limitations, an efficient modification to the existing scheme is proposed using an affine Hill cipher in combination with ECC and a 3D chaotic map. The efficiency of the modified scheme is demonstrated through experimental results and numerical simulations.

Keywords: affine Hill cipher; brute force attack; cryptanalysis; elliptic curve; Kerckchoff's principle; 3D Arnold transform

MSC: 68P25; 94A60

Citation: Lone, P.N.; Singh, D.; Stoffová, V.; Mishra, D.C.; Mir, U.H.; Kumar, N. Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher. *Mathematics* **2022**, *10*, 3878. https://doi.org/10.3390/math10203878

Academic Editor: Antanas Cenys

Received: 24 September 2022
Accepted: 17 October 2022
Published: 19 October 2022

1. Introduction

Modern day technology is highly interlinked with digital communication over the internet, however, the privacy of data during transmission is a highly important issue. For instance, when using multimedia for e-business, military organization, medical purposes, education, meteorology, space organization, etc., privacy and security are of the utmost interest [1]. Thus, due to the immense threat posed by hackers and hacking tools, there is an ongoing need for efficient cryptographic techniques to protect sensitive information provided over open network channels. In response to this need, a number of symmetric and asymmetric cryptographic techniques are in use to safeguard sensitive information. ECC is one of the newest and most popular asymmetric approaches used to support encryption techniques. The primary advantage of ECC lies in the fact that it is hard to solve the underlying elliptic curve discrete logarithm problem (ECDLP). Furthermore, owing to its shorter key length, ECC systems are more demanding and widely applicable. It is imperative to mention that the RSA system provides security with a 1024–3072 bit-length key, whereas ECC provides the same security with only a 160–256 bit-length key [2]. ECC has gained a respectable status among cryptographic researchers due to its low memory use, bandwidth savings, and lower power consumption in hardware implementations [3–5]. Digital images need to be securely transferred over communication channels while considering a reliable encryption scheme. Despite several advantages of ECC in image encryption,

several issues must be considered before designing a cryptosystem, viz. key size, key space, and the chosen elliptic curve. The primary focus of encryption schemes is to enhance key strength in order to resist an exhaustive key search attack. If proper attention is paid when choosing elliptic curves, then the best known attacks are considerably weaker against solving ECDLP compared to the best algorithms for solving the discrete logarithm problem [6].

Recently, Dawahdeh et al. [7] proposed an encryption scheme combining the elliptic curve and Hill cipher techniques. This scheme is mainly intended to protect image data while ensuring fast transmission of highly correlated multimedia data. The idea underlying the said scheme is to change the Hill cipher technique from symmetric to asymmetric using the generated parameters of ECC to develop the secret key. However, there is a serious loophole in the existing scheme in the form of secret keys, which makes it vulnerable to brute force attacks.

The use of ECC in combination with other symmetric techniques has been widely used in image and text encryption schemes [2,8–13]. In [8], the authors presented an efficient cryptosystem using an elliptic curve over finite rings in combination with S-boxes. The scheme in [12] proposed text encryption that could encrypt any script with defined ASCII values by making use of elliptic curves. Moreover, in [9] the authors made use of elliptic curves to simultaneously encrypt and compress multimedia data. On the other side, for instance, in Khoirom et al. [14], used cryptanalysis against the scheme in [9] to expose the secret key from the public key. Furthermore, Abd El-Latif et al. [10] presented an algorithm using a chaotic map and the elliptic curve which, while it seemed difficult to hack due to the complex structure of key generators, was broken through cryptanalysis by Hong et al. [15]. In this paper, cryptanalysis of the scheme proposed in [7] is carried out, revealing that the strength of the secret key can be easily broken through an exhaustive key search. Due to the linearity of the Hill cipher, it is vulnerable against smaller key spaces. Furthermore, the same weaker secret key is used to generated the self-invertible matrix, and is used for both encryption and decryption.

In this work, we examine the security of the scheme in [7] and develop a corresponding efficient and improved version for greater security of image data. Keeping in mind that ECC and affine Hill ciphers are popular encryption techniques that can provide better performance and higher levels of security, we revamp the existing scheme by replacing the Hill cipher by an affine Hill cipher in the key domain of $\mathbb{SL}_m(\mathbb{F}_p)$ and $\mathbb{M}_m(\mathbb{F}_p)$. Furthermore, the confusion and diffusion architecture of the scheme is covered via a 3D Arnold map using ECC and bit-wise XOR operations. In addition, the chaotic behavior of this novel scheme makes it more efficient, unpredictable, and strong in resisting illicit hackers [16,17]. Thus, systems modified with chaotic maps shows more efficacy than the normal symmetric and asymmetric systems. It is appropriate to mention that higher-dimensional chaotic maps are known for their high quality of encryption. In this direction, a combination of a private and a public technique is used to design a secure algorithm for image encryption in the presence of higher-dimensional chaotic maps [18]. The numerical outcomes demonstrate the efficiency and stalwartness of the proposed scheme. Furthermore, detailed comparisons with existing schemes [7,9,10,13,19,20] serve to validate the higher efficiency and security of the proposed scheme.

The outline of the article is as follows: Section 2 presents the basic mathematical theories involved; Section 3 highlights the encryption scheme of the cryptosystem [7]; in Section 4, the cryptanalysis of the scheme [7] and its improvement are explained; and Section 5 presents a demonstration of the improved version. Finally, experimental analysis is carried out in Section 6, detailed numerical simulations are presented in Section 7, and the conclusions of the work are presented in Section 8.

2. Basic Theories

2.1. Mathematical Concept Of Elliptical Curves

Let $q > 3$ be a prime number, and let $\mathbb{F}_q$ be a field of integers modulo q. The elliptic curve $\mathbb{E}$ is an algebraic curve defined as the set of all pairs $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ satisfying Equation (1), defined as follows:

$$\mathbb{E} : y^2 = x^3 + ax + b, \tag{1}$$

with an imaginary point at infinity denoted by $\mathcal{O}$, where, $a, b \in \mathbb{F}_q$ such that $4a^3 + 27b^2 \not\equiv 0 \pmod{q}$. The discriminant condition indicates that the curve is non-singular, that is, it has no self-intersections or vertices. The set of all the points on the curve forms a finite Abelian group with $\mathcal{O}$ as an identity element. The elliptic curve over some finite field $\mathbb{F}_q$ is denoted by $\mathbb{E}_q(a, b)$ and is a special type of polynomial equation [2,6]. Elliptic curve operations such as point addition, point doubling, and point multiplication are discussed in [7], and examples of elliptic curves over $\mathbb{R}$ are shown in Figure 1.

Elliptic Curve Diffie–Hellman Key Exchange (ECDH) is an advanced analogy to Diffie–Hellman Key Exchange. In the modified proposed algorithm, the secret keys of a 3D Arnold map are shared through an ECDH scheme. The representation of key exchange can be performed similarly to the Diffie–Hellman protocol, and it is a relatively difficult task to find a suitable elliptical curve. The curve should satisfy certain conditions, as discussed above, in order achieve good security. The exchange of the key parameters between user A and user B can be achieved using the following steps ((i)–(v)):

(i) **Public element:** Select an elliptic curve $\mathbb{E}_q(a, b)$ with the parameters $a, b \in \mathbb{F}_q$, with q a large prime of at least 160-bit length and a generator point G of order r, i.e., $rG = \mathcal{O}$ on the elliptic curve.

(ii) **User A Generate:** Select a random private key $\eta_A \in [1,\ q-1]$ and calculate $P_A = \eta_A G$

(iii) **User B Generate:** Select a random private key $\eta_B \in [1,\ q-1]$ and calculate $P_B = \eta_B G$

(iv) **User A calculate secret key:** $K = \eta_A \times P_B$

(v) **User B calculate secret key:** $K = \eta_B \times P_A$

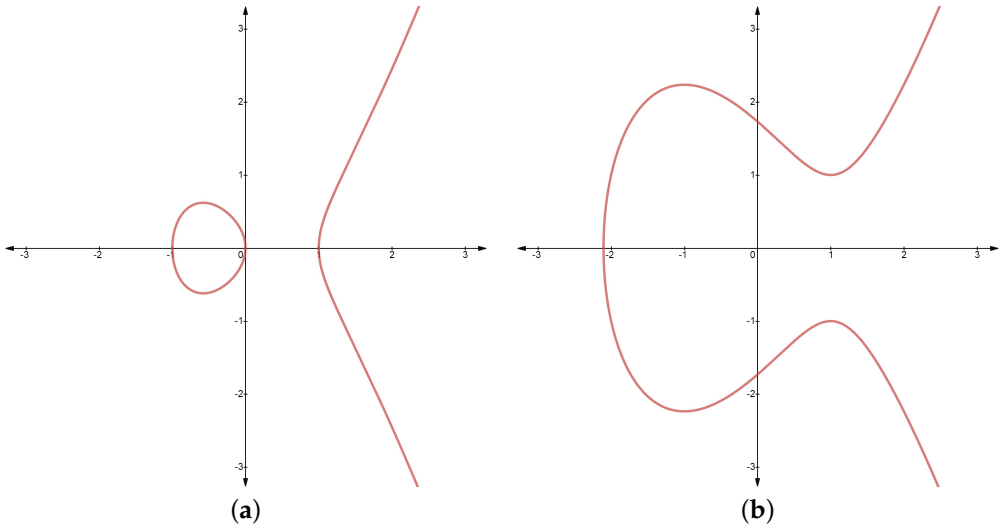

Figure 1. Elliptic curves over $\mathbb{R}$. (**a**): Elliptic curve for $y^2 = x^3 - 3x + 3$ over $\mathbb{R}$, and (**b**): Elliptic curve for $y^2 = x^3 - x$ over $\mathbb{R}$.

2.2. Affine Hill Cipher

An affine Hill cipher is a classical symmetric cipher suitable for encryption schemes, and is defined as follows: $AX + B$, here $A \in \mathbb{SL}_m(\mathbb{F}_p)$ and $B \in \mathbb{M}_m(\mathbb{F}_p)$, are the secret key

parameters of the same size as the generated blocks of X. The key elements of an affine Hill cipher are chosen from $\mathbb{SL}_m(\mathbb{F}_p)$, called a special linear group of matrices over some finite field $\mathbb{F}_p$, while $\mathbb{M}_m(\mathbb{F}_p)$ is called a group of matrices over some finite field $\mathbb{F}_p$ of order m, and is used to provide a larger key space. Mathematically, $\mathbb{SL}_m(\mathbb{F}_p)$ is a subgroup of a general linear group of matrices $\mathbb{GL}_m(\mathbb{F}_p)$, and is defined in Equation (2):

$$\mathbb{SL}_m(\mathbb{F}_p) = \{A \in \mathbb{GL}_m(\mathbb{F}_p) \mid \det(A) = 1\}. \tag{2}$$

with cardinality equal to

$$|\mathbb{SL}_m(\mathbb{F}_p)| = \tfrac{1}{p-1} \prod_{i=0}^{m-1} (p^m - p^i).$$

Furthermore, the group of matrices over some finite field $\mathbb{F}_p$ is defined in Equation (3):

$$\mathbb{M}_m(\mathbb{F}_p) = \{A \in [a_{i,j}]_{m \times m} \mid a_{i,j} \in \mathbb{F}_p\}, \tag{3}$$

with cardinality equal to

$$|\mathbb{M}_m(\mathbb{F}_p)| = p^{m^2}.$$

The affine Hill cipher for block matrices of order $m \times m$ is defined in Equation (4):

$$E_{m \times m} = S_{m \times m} B_{m \times m} + M_{m \times m} \pmod{256}, \tag{4}$$

where, $S_{m \times m} \in \mathbb{SL}_m(\mathbb{F}_p)$ and $M_{m \times m} \in \mathbb{M}_m(\mathbb{F}_p)$ are the two key parameters, $B_{m \times m}$ is the original data block, and $E_{m \times m}$ is the encrypted block.

The 3-D Arnold Map

The chaos 3D Arnold transform defined in Equation (5) is used by extending the classical 2D Arnold transform defined in Equation (6) [21]:

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} 1 & a_1 & 0 \\ a_2 & a_1 a_2 + 1 & 0 \\ a_3 & a_4 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \bmod (n), \tag{5}$$

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a_1 \\ a_2 & a_1 a_2 + 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \tag{6}$$

where, (x', y', z') are modified values and the parameters a_1, a_2, a_3 and a_4 are chosen from the curve $\mathbb{E}_p(a, b)$. The 3D Arnold map is chaotic in nature, and is one of the finest members of the higher-dimensional chaotic maps used for the scrambling process [22].

In this approach, dual encryption by Arnold transform is achieved by permutation and substitution. The transform is simplified, as defined in Equation (7):

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a_1 \\ a_2 & a_1 a_2 + 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod (n), \quad z' = a_3 x + a_4 y + z \bmod (m), \tag{7}$$

where, n is the image size, m represents the gray levels, and z' is a one-dimensional array of length n used to further enhance the diffusion using bit-wise XOR operation.

3. Scheme Proposed by Dawahdeh et al. [7]

The scheme in [7] presents a cryptosystem designed through the ECC and Hill cipher technique. The secret key for a Hill cipher is obtained from ECC, and later an involuturay matrix is generated from the shared key to be used for both encryption and decryption [23]. Before encryption, both parties should agree on the elliptic curve parameters $\{q, a, b, G\}$, where, G is one of the generating points of the curve. The sender and receiver choose their

private keys η_A, η_B from the domain $[1, q-1]$, and can generate their corresponding public keys $P_A = \eta_A G$ and $P_B = \eta_B G$ over $\mathbb{E}_q(a, b)$, respectively. The encryption scheme in [7] is described through Algorithms 1 and 2.

Algorithm 1: Elliptic curve key generation over some $\mathbb{E}_q(a, b)$.

▷ Input:$\{\eta_A, q, a, b, P_B, G\}$ ▷ Output:(a_1, a_2, a_3, a_4)

1. Compute $(x, y) \leftarrow \eta_A P_B$; // Elliptic curve operation
2. Compute $(a_1, a_2) \leftarrow xG = (x_1, y_1)$; // Elliptic curve operation
3. Compute $(a_3, a_4) \leftarrow yG = (x_2, y_2)$; // Elliptic curve operation
4. Generate $K = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$;

Algorithm 2: Encryption algorithm of the scheme [7].

▷ Input: $P_{i,j}$ (plain image of size $m \times n$), K (key obtained from algorithm 1). ▷ Output: $C_{i,j}$ (cipher image)

1. Compute $K_m = \begin{bmatrix} K & I - K \\ I + K & -K \end{bmatrix}_{4\times 4}$; // K_m stores a key matrix of order 4
2. **for** i = *1:length*$(\frac{mn}{4})$ **do**
   $P^i_{4\times 1} \leftarrow$ **Gen_blocks**$(P_{i,j})$; // Split image into blocks of size 4×1
3. **for** i = *1:length*$(\frac{mn}{4})$ **do**
   $C^i_{4\times 1} \leftarrow$ **Compute**$(K_m \times P^i_{4\times 1})(\text{mod } 256)$; // Use of Hill cipher
4. **for** i = *1:length*$(\frac{mn}{4})$ **do**
   $C_{i,j} \leftarrow$ **Gen_cipher**$(C^i_{4\times 1})$; // Concatenate the image blocks to original size

4. Cryptanalysis and Improvement

Cryptanalysis is the breakdown of codes through different cryptanalytic attacks. The hardness of ECC lies in ECDLP, as solving such an algorithm is computationally infeasible. The authors convert the Hill cipher technique from symmetric to asymmetric in order to operate the scheme using a shared secret key. The scheme in [7] suggests large primes for higher security of the shared key (x, y) over $\mathbb{E}_q(a, b)$. The ordered pairs $xG = (x_1, y_1)$ and $yG = (x_2, y_2)$ are generated over $\mathbb{E}_q(a, b)$ to form the key matrix K_m, which is vulnerable and could be collapsed by a brute force attack.

4.1. Brute Force Attack on the Scheme in [7]

A brute force attack is a classical cryptanalysis approach which tests all the possible sets of keys by treating the encryption method as a black box [6]. The security of the scheme in [7] lies in xG and yG. Because Equation (8) reveals the same results for large primes q,

$$[K_m(\text{mod } q)P^i](\text{mod } 256) \equiv K_m P^i(\text{mod } 256). \tag{8}$$

As K_m is generated from K and P^i is the plain text block, this implies that it is only necessary to to find x_i, y_i; $i = 1, 2$ under modulo 256. Because each parameter is eight bits, a total possible choice to find through exhaustive key search is of length 2^{32}, i.e., only 4,294,967,296 matrices of order 2, which is vulnerable to brute force attacks through modern high-speed technology. To resist such a brute force attack, the key space of the image encryption scheme should be larger than 2^{128} [24,25]. Thus, the brute force attack can successfully estimate 56–64 bit length within a few hours or a day [6]. Even the COPA-COBANA (Cost-Optimized Parallel Code Breaker) machine can break such an algorithm in less than a day, and its computational power is up to 64 bits [26]. Jack, in [27], breaks down the Hill cipher for $n = 2$ with an IBM 650 machine, and finds it impractical and highly complex for higher values of n. The same is the case here; the only unknowns are x_i, y_i; $i = 1, 2$ under modulo 256 of bit length 2^{32}, and no confusion of pixel values

is present, thus, such a system can possibly hacked or collapsed through contemporary high-speed technology.

4.2. Improvement

The limitations of the scheme are that it lacks the confusion property and smaller key space. Thus, the scheme can be upgraded to include the confusion and diffusion properties with an enlarged key space in order to fill the accessible gap of the extant scheme [7].

A modified and improved version of the existing scheme is presented using ECC and an affine Hill cipher in a chaotic environment to adjust the major limitations of the scheme in [7]. To extend the key space, a group of involuntary matrices are replaced by a $\mathbb{SL}_m(\mathbb{F}_p)$ and $\mathbb{M}_m(\mathbb{F}_p)$ domain over some finite field $\mathbb{F}_p$ to achieve a higher level of diffusion in the scheme. Furthermore, a chaos map is employed in the scheme to scramble all the positions of the image by choosing the key parameters from the public domain $\mathbb{E}_q(a, b)$.

5. Proposed Methodology of the Improved Scheme

An improved encryption scheme is proposed to secure communication of images over public channels. In this scheme, 4×4 blocks are generated from the original image matrix and then diffused by an affine Hill cipher using the key matrices chosen from $\mathbb{SL}_m(\mathbb{F}_p)$ and $\mathbb{M}_m(\mathbb{F}_p)$, where, $m = 4$ and p are a prime number of at least 8 bits in length. Furthermore, the key parameters for the chaotic map are generated from the chosen elliptic curve $\mathbb{E}_q(a, b)$ over some finite field $\mathbb{F}_q$ to scramble the position of pixels, and over the scrambled values a bit-wise XOR operation is performed with the generated Arnold map sequence, as discussed in Algorithm 3.

Algorithm 3: PROPOSED ENCRYPTION SCHEME

► **Input** : I_{ij} (plain image), $k_1 \in \mathbb{SL}_4(\mathbb{F}_p)$, $k_2 \in \mathbb{M}_4(\mathbb{F}_p)$ and η_A, q, a, b, P_B, G.
► **Output**: C_{ij} (cipher image)

After segregation of color planes $\{I_r, I_g, I_b\}$ from plain image.
$I^i_{r,g,b} \leftarrow$ **Split**(I_r, I_g, I_b, 4); // Split each image into 4×4 blocks
for *i* ← *1:length(i)* **do**
  $B^j_M \leftarrow$ **Mul_block**($I^i_{r,g,b}$,k_1); // Multiplication of each block with key k_1
end
for *i* ← *1:length(i)* **do**
  $B^i_A \leftarrow$ **Add_block**(B^j_M, k_2); // Addition of each block with key k_2
end
$B^j \leftarrow$ **Merge_block**(B^i_A) // Concatenate the image blocks back to original size
$K \leftarrow$ **Key_generation**(η_A, q, a, b, P_B, G); // Generate key K by using algorithm 1
$B^j \leftarrow$ **Scramble_Ard**(B^j, a_1, a_2); // Shuffling of pixels using chaotic map
for *i* ← *1:length(B^j)* **do**
  $X_i \leftarrow$ **generate_seq_Ard**(a_3, a_4); // Sequence generation for Xor operation
end
$X_i \leftarrow$ **Reshape**(X_i); // Shaping generated sequence into a matrix
for $i \leftarrow 1 : length(B^j)$ **do**
  $C^j \leftarrow$ **Bit_xor(**B^j, X_i**)**;// Xor operation
end
$C_{ij} \leftarrow$ **Concat(**B^j**)**; // Concatenate R, G, B image planes **Output** : C_{ij}(cipher image).

6. Experimental Results

The results described in this section were obtained in Matlab 2020a with a Core-i3 supporting environment with 4 GB RAM on a Windows 7 system. The images were chosen from USC-SIPI databases. The experimental results are shown in Figures 2–4.

Figure 2. Original images on which the proposed algorithm was tested: (**a**) Jet, (**b**) Home, (**c**) Barbara, (**d**) Baboon, (**e**) Pepper, (**f**) Lady.

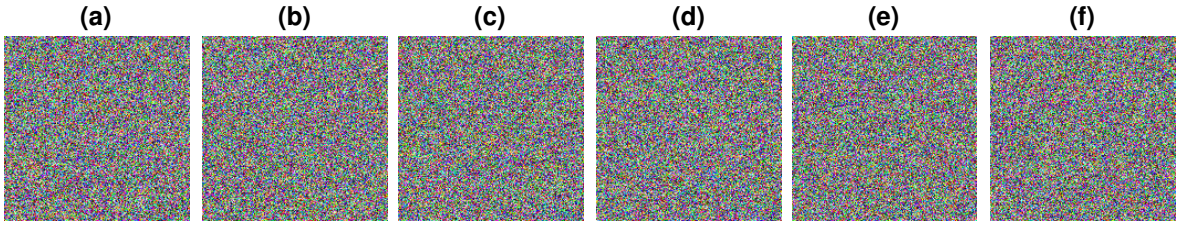

Figure 3. Respective encrypted images of the image set shown in Figure 2. (**a**) Jet, (**b**) Home, (**c**) Barbara, (**d**) Baboon, (**e**) Pepper, (**f**) Lady.

Figure 4. Respective decrypted images of the corresponding encrypted images shown in Figure 3. (**a**) Jet, (**b**) Home, (**c**) Barbara, (**d**) Baboon, (**e**) Pepper, (**f**) Lady.

7. Security Analysis

7.1. Key Space Analysis

The key space is the set of all possible choices that can be used to encrypt an image. Thus, schemes with a larger key space support greater robustness against exhaustive key search attacks. In the proposed scheme, factors supporting the key space are the elements of $\mathbb{SL}_m(\mathbb{F}_p)$, $\mathbb{M}_m(\mathbb{F}_p)$, and the parameters of the Arnold map shared through ECC. The total for the key space is summarized below:

- The choices for $\mathbb{SL}_m(\mathbb{F}_p)$ during the encryption process are defined as follows:

$$|\mathbb{SL}_m(\mathbb{F}_p)| = \frac{1}{p-1}\prod_{i=0}^{m-1}(p^m - p^i). \tag{9}$$

- $\mathbb{M}_m(\mathbb{F}_p)$ works as an additive key element in the affine Hill cipher, with possible choices p^{m^2}.
- The publicly shared parameters for the Arnold map through ECC can be reduced up to 256^4 choices.

Thus, the size of generalised key space is defined by Equation (10):

$$|\mathbb{SL}_m(\mathbb{F}_p)||\mathbb{M}_m(\mathbb{F}_p)|(256^4) = \left(\tfrac{1}{p-1}\textstyle\prod_{i=0}^{m-1}(p^m - p^i)\right)(p^{m^2})(256^4). \tag{10}$$

The keyspace defined in Equation (10) is strong enough against brute force attacks. For experimental results, we have chosen $m = 4$ and $p = 223$, for an approximate key space

of $10^{82} = 2^{272}$, which is large enough to resist brute force attacks. Thus, the scheme is be appropriate for secure communication purposes.

7.2. Key Sensitivity

After achieving confusion and diffusion in a scheme, the sensitivity of keys is necessary to check the security of an algorithm. In this scheme, the sensitivity of an algorithm is checked in the worst-case scenario when parameters are 99% known with a bit change in key parameters. The sensitivity results for different cases of the algorithm are shown in Figures 5 and 6, and are sufficient to support the sensitivity of the algorithm. The change in 3D Arnold key parameters at both stages of confusion through shuffling and the diffusion through XOR operation are shown in Figures 5c,d and 6c,d. Furthermore, a marginal change in multiplicative parameters are shown in Figures 5e and 6e and the additive parameters of the affine Hill cipher are shown in Figures 5f and 6f.

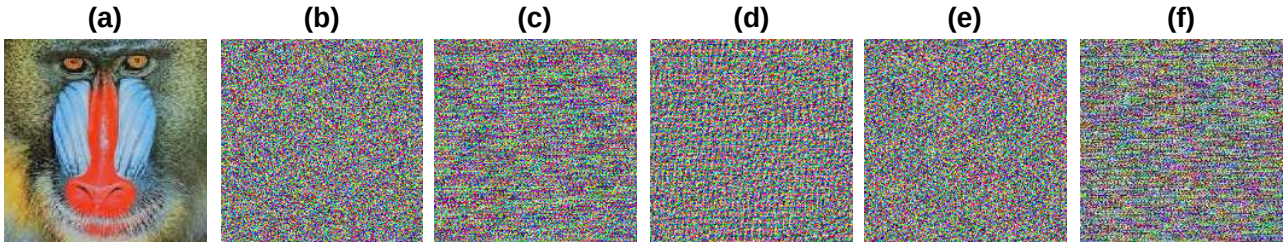

Figure 5. Sensitivity analysis of the image in Figure 2d: (**a**) original image, (**b**) cipher image, (**c**–**f**) decrypted images with a bit change in the secret key parameters.

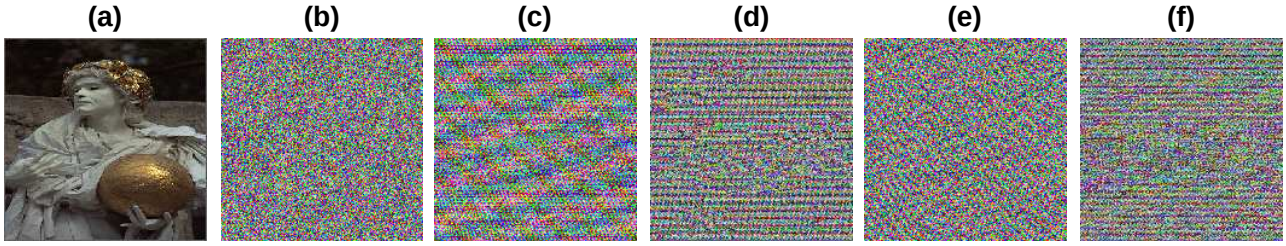

Figure 6. Sensitivity analysis of the image in Figure 2f: (**a**) original image, (**b**) cipher image, (**c**–**f**) decrypted images with a bit change in the secret key parameters.

7.3. Histogram Analysis

A histogram analysis is a graphical representation between pixel values and the intensity values of the data to present the frequency distribution information. A secure and good encryption scheme produces the evenly distributed data of the cipher images. The results of the test images are shown in Figures 7–11. The distribution plot of the cipher images shows a uniform distribution, implying that the encrypted data are secure and that such an algorithm cannot leak information to outsiders.

Now, the uniformity of the data through the chi-square test can be ensured using Equation (11):

$$\chi^2 = \sum_{k=0}^{2^n-1} \frac{(\mathcal{O}_k - \mathcal{E}_k)^2}{\mathcal{E}_k}, \tag{11}$$

where, $\mathcal{O}_k$ and $\mathcal{E}_k = \frac{mn}{256}$ are the observed and expected frequency, respectively, of an image with size mn. At significance level $\alpha = 1\%$ and $\alpha = 5\%$ with 255 degrees of freedom, the critical chi-square values to pass the hypothesis uniformity are $\chi^2_{(0.01,255)} = 310.4574$ and $\chi^2_{(0.05,255)} = 293.2478$, respectively. Table 1 shows the chi-square values on a set of images at significance levels of 1% and 5%.

Table 1. χ^2-values of the scheme.

Cipher Image	χ^2 Values				H_0
	R	G	B	Average	
Jet	284.2314	218.6172	232.1876	245.0120	accept
House	223.2356	286.2349	267.2496	258.9067	accept
Barbara	262.1451	258.2149	287.2350	269.1983	accept
Baboon	289.2571	267.8561	300.2225	285.7785	accept
Pepper	279.1311	297.2389	299.2314	291.8671	accept
Lady	252.1421	289.1563	301.4568	280.9184	accept

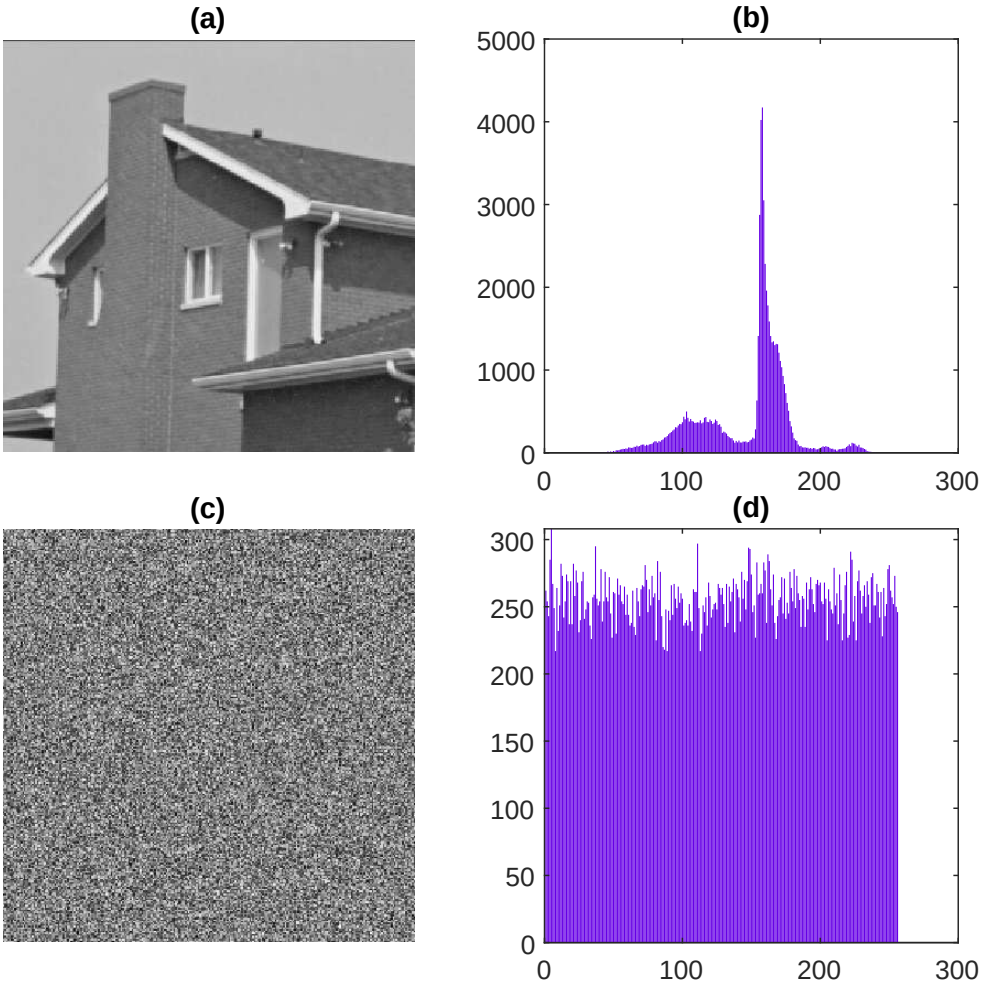

Figure 7. Histogram analysis of grayscale image: (**a**) input image, (**b**) histogram of input image, (**c**) encrypted images, (**d**) histogram of encrypted image.

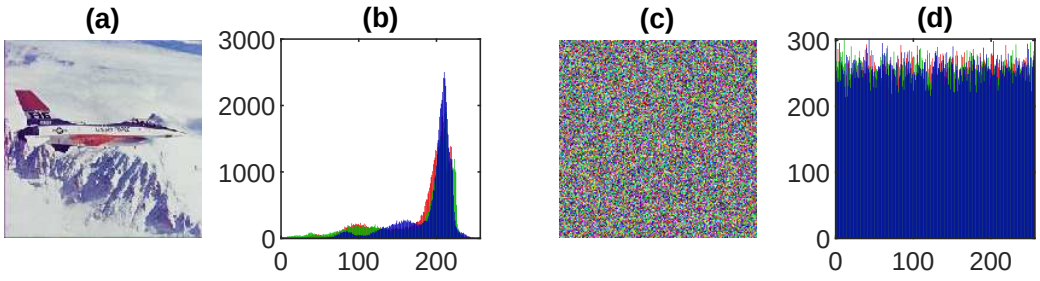

Figure 8. Histogram analysis of the image in Figure 2a: (**a**) the original image, (**b**) histogram of the original image, (**c**) encrypted image, (**d**) histogram of the encrypted image.

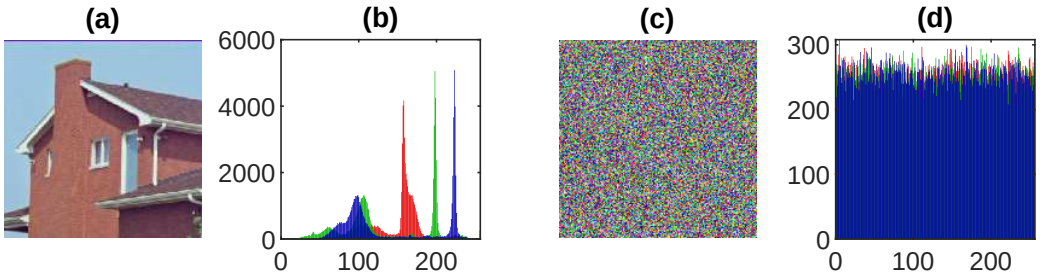

Figure 9. Histogram analysis of the image in Figure 2b: (**a**) the original image, (**b**) histogram of the original image, (**c**) encrypted image, (**d**) histogram of the encrypted image.

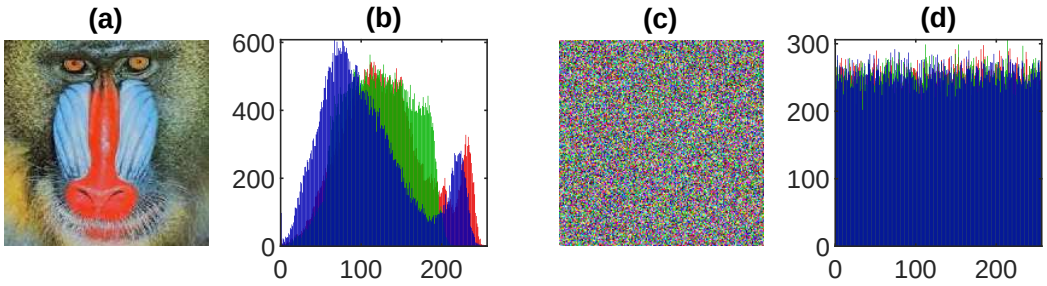

Figure 10. Histogram analysis of the image in Figure 2d: (**a**) the original image, (**b**) histogram of the original image, (**c**) encrypted image, (**d**) histogram of the encrypted image.

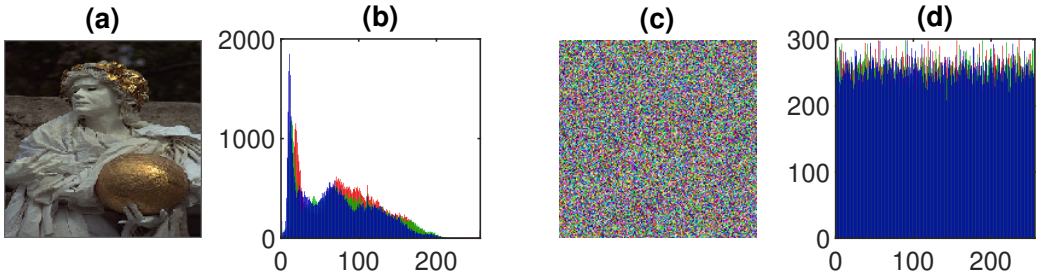

Figure 11. Histogram analysis of the image in Figure 2f: (**a**) the original image, (**b**) histogram of the original image, (**c**) encrypted image, (**d**) histogram of the encrypted image.

7.4. Correlation Analysis

Correlation refers to the relationship between adjacent pixels. Thus, in plain images a strong correlation among the pixels is found with a dense correlation graph, while in cipher images a low correlation among the adjacent pixels with an evenly distributed graph is found. The correlation for input and cipher images in the horizontal (H), vertical (V) and diagonal (D) directions is presented in Figure 12.

Furthermore, the correlation graphs of the images and their corresponding cipher images in different directions are shown in Figure 12. From Figure 12, it can be seen that the correlation graph of cipher images is uniformly distributed throughout the domain, with an ideal value of correlation coefficient in all directions shown in Tables 2 and 3. The equation used to calculate the correlation coefficient value is taken as given in Equation (12).

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\frac{1}{N}\sqrt{\sum_{i=1}^{N}[x_i - E(x)]^2 \sum_{i=1}^{N}[y_i - E(y)]^2}}, \tag{12}$$

where,

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][(y_i - E(y)], \tag{13}$$

and

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{14}$$

where, N is number of pixels, $E(x)$ is the expectation, and $D(x)$ is the variance.

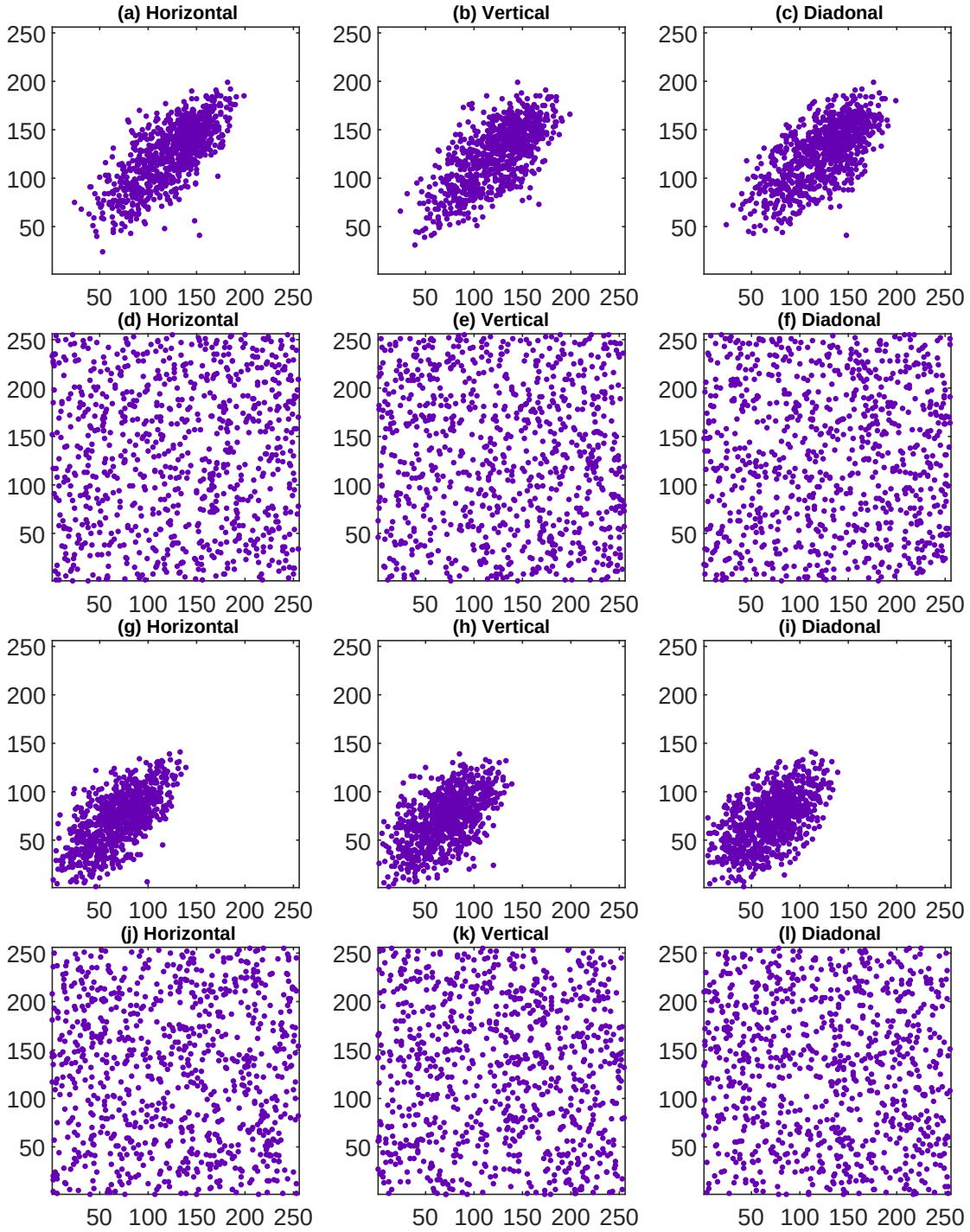

Figure 12. Correlation analysis of grayscale images: (**a**–**c**) shows the correlation of the input image jet.jpeg, (**d**–**f**) shows the correlation of the cipher image of jet.jpeg, (**g**–**i**) shows the correlation of the input image baboon.jpeg, (**j**–**l**) shows the correlation of the cipher image of baboon.jpeg. All images include the horizontal, vertical, and diagonal directions.

Table 2. Correlation results for the input and cipher images.

Images	Input			Cipher		
	H	**V**	**D**	**H**	**V**	**D**
Jet	0.9231	0.9568	0.9425	0.0002	−0.0024	0.0026
House	0.9654	0.9452	0.9624	−0.0019	0.0001	0.0029
Barbara	0.9568	0.9214	0.8745	0.0017	−0.0020	0.0047
Baboon	0.8469	0.8456	0.8989	0.0021	0.0011	0.0011
pepper	0.8548	0.8791	0.9399	0.0004	0.0019	0.0003
Lady	0.9269	0.9765	0.9578	0.0023	0.0041	0.0014

Table 3. Comparison results of the correlation coefficient with existing techniques.

Methods	Input			Cipher		
	H	**V**	**D**	**H**	**V**	**D**
Proposed	0.9123	0.9207	0.9293	0.0008	0.0004	0.0021
Ref. [10]	0.9473	0.9544	0.9122	0.0010	0.0017	0.0125
Ref. [13]	0.9326	0.9624	0.9097	0.0035	−0.0040	−0.0410
Ref. [19]	0.9487	0.8994	0.8734	0.0000	0.0004	−0.0009
Ref. [20]	0.9677	0.9829	0.9532	0.0719	−0.3188	−0.0017

7.5. Quality Measure

The parameters used to measure the quality between plain images and cipher images are as follows [19].

7.5.1. Mean Square Error (MSE)

The MSE is calculated between the input and the output image using Equation (15). The results shown in Table 4 support the robustness of the proposed algorithm:

$$\text{MSE} = \frac{1}{NM}\sum_{i}^{N}\sum_{j}^{M}(I_p(i,j) - I_c(i,j)), \tag{15}$$

where, I_p and I_c are the input and output image, respectively, of size NM.

7.5.2. Peak Signal to Noise Ratio (PSNR)

PSNR is a quality measure between input and output images using Equation (16). A good level of encryption is identified when PSNR is less than 10 db. The calculated test values of PSNR are demonstrated in Table 4:

$$\text{PSNR} = 10\log_{10}\left(\frac{2^n - 1}{\text{MSE}}\right), \tag{16}$$

where, n is the bits per pixel and MSE is as defined in Equation (15).

7.5.3. Structural Similarity Index (SSIM)

The SSIM is a measure of the input and output image that checks the quality of the encryption algorithm. The SSIM values should be approximate to zero for the output images for a secure algorithm, and can be calculated using Equation (17), defined below:

$$\text{SSIM(p,c)} = \frac{(2\mu_p\mu_c + c)(2\sigma_{pc} + c')}{(\mu_p^2 + \mu_c^2 + c)(\sigma_p^2 + \sigma_c^2 + c')}), \tag{17}$$

where, σ_{pc}, (μ_p, μ_c), and (σ_p, σ_c) are the covariance, mean, and standard deviation of the plain and cipher images, respectively. Moreover, c and c' are the variables to be stabilized.

The experimental values are provided in Table 4, and are close to the ideal value of zero.

Table 4. Quality measures between input images and output images.

Images	MSE			PSNR			SSIM		
	R	G	B	R	G	B	R	G	B
Jet	4.192×10^4	7.180×10^4	8.993×10^3	8.145	7.547	7.128	0.002	0.005	0.005
House	9.941×10^3	6.120×10^4	8.973×10^3	8.254	8.548	8.489	0.001	0.000	0.001
Barbara	1.257×10^4	9.180×10^3	7.257×10^4	8.189	9.512	8.178	0.009	0.006	0.008
Baboon	9.256×10^3	8.595×10^3	8.980×10^4	6.235	7.249	6.954	0.006	0.001	0.003
Pepper	8.120×10^4	1.235×10^4	4.985×10^3	9.517	8.865	8.562	0.002	0.000	0.002
Baboon	9.456×10^3	8.156×10^3	9.562×10^3	7.214	9.121	8.128	0.001	0.002	0.001

7.6. Differential Attack Analysis

A differential attack is a type of cryptanalysis used to analyze secret keys through different cipher images. In this approach, a small modification is carried out on the pixel intensity values of the original images to attempt to find the difference between the corresponding cipher images in order to observe the relationship between the plain and cipher images. The differential measurements used to find the resilience of the system through the number of the pixel change rate (NPCR) and unified average changing intensity (UACI) are defined in Equations (18) and (19):

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{\text{T}} \times 100\%, \tag{18}$$

$$\text{UACI} = \frac{1}{\text{T}} \sum_{i,j} \left(\frac{C_1(i,j) - C_2(i,j)}{255} \right) \times 100\%, \tag{19}$$

where, T is the total size of the image, C_1 and C_2 are cipher images differing by a single pixel value, and $D(i,j)$ is defined as

$$D(i,j) = \begin{cases} 1, & if\ C_1(i,j) \neq C_2(i,j), \\ 0, & \text{elsewere}, \end{cases}$$

For analysis, the computed results are provided in Table 5 and compared in Table 6. The test values approximate the ideal values of NPCR (99.6094%) and UACI (33.4635%), demonstrating that the improved algorithm is robust against such attacks.

Table 5. NPCR and UACI results for the color plane the of cipher image.

Images	NPCR				UACI			
	R Layer	G Layer	B Layer	Average	R Layer	G Layer	B Layer	Average
Jet	99.5832	99.6321	99.6154	99.6102	33.4425	33.3901	33.3956	33.4049
House	99.6039	99.6412	99.6423	99.6294	33.4213	33.3452	33.2845	33.3503
Barbara	99.6234	99.6481	99.6321	99.6345	33.3425	33.3614	33.3329	33.3456
Baboon	99.6231	99.5931	99.6548	99.6236	33.2956	33.2814	33.3621	33.3130
Pepper	99.6513	99.6059	99.6623	99.6398	33.2956	33.3521	33.3089	33.3188
Lady	99.5956	99.5759	99.5973	99.5896	33.4732	33.4623	33.3993	33.4449

Table 6. Comparison of NPCR and UACI results.

Methods	Image	NPCR	UACI
Proposed	Barbara	99.6345	33.3456
Ref. [7]	(256×256)	–	30.4814
Ref. [9]	(256×256)	99.2996	33.5844
Ref. [19]	(256×256)	99.6220	33.5268
Ref. [10]	(256×256)	99.5	33.3

7.7. Shannon's Entropy Analysis

The Shannon's entropy is proportional to the measure of uncertainty. The ideal entropy value of random data is 8 [28]. Thus, an efficient encryption scheme has an entropy value that approximates the ideal value and is uniform with the gray values of the image. In Table 7, entropy values are shown for different images as calculated by Equation (20):

$$\text{Entropy} = \sum_{i=0}^{2^n-1} p(m_i) \log_2 \left(\frac{1}{p(m_i)} \right), \tag{20}$$

where, $p(m_i)$ is the probability of source m_i.

Table 7 and Figure 13 show the calculated entropy values of the input and output images; the values approximate the ideal value, which is a strong indication of the randomness and security of the data. Thus, the improved version of the scheme achieves a perfect level of permutation to secure the secret information. Furthermore, Tables 8 and 9 compare the entropy results with existing several schemes, and the results justify the security of the proposed scheme against entropy attacks.

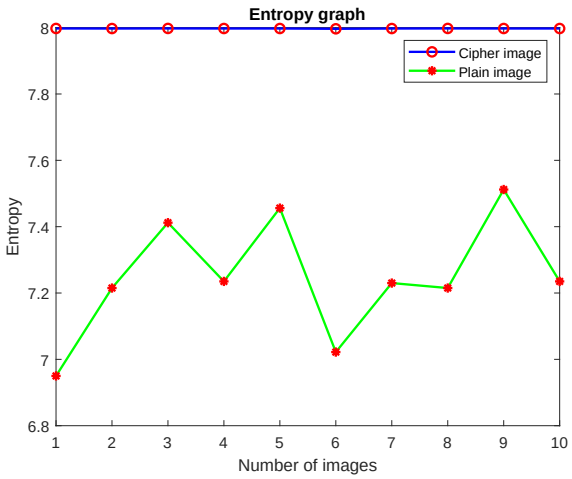

Figure 13. Entropy graph of input images and their cipher images.

Table 7. Entropy value of cipher images.

Images	Entropy			Average
	R	G	B	
Jet	7.9978	7.9979	7.9978	7.9978
Home	7.9979	7.9977	7.9979	7.9978
Barbara	7.9979	7.9979	7.9979	7.9979
Baboon	7.9979	7.9978	7.9978	7.9978
Pepper	7.9976	7.9975	7.9977	7.9976
Lady	7.9975	7.9978	7.9975	7.9976

Table 8. Comparison of entropy results.

Method	Image	Entropy
Ref. [7]	(256 × 256)	7.9970
Ref. [9]	(256 × 256)	7.9969
Ref. [10]	(512 × 512)	7.9973
Ref. [19]	(256 × 256)	7.9974
Ref. [20]	(512 × 512)	5.3390
Proposed	Barbara (256 × 256)	7.9979

Table 9. Statistical measures of grayscale cipher images.

Images (256×256)	Entropy	PSNR	UACI
Home	7.9982	7.4523	33.1245
Barbara	7.9979	7.1133	33.2814
Baboon	7.9979	6.1576	33.7852
Pepper	7.9983	7.4121	33.3089
Average	7.9983	7.4121	33.3089
Ref. [7]	7.9970	8.5777	30.4817
Ref. [11]	–	7.6568	34.0998

7.8. Noise Attacks

Due to effects from the transmission channels, the data may be affected by noise signals.

To check the effect of noise on the sensitivity of information, different noise effects on the data can be used to check the resistance of the algorithm against noise attacks. A number of noise techniques are available to check this, such as salt and pepper and Gaussian noise in different proportions. Thus, Figures 14 and 15 show the noise-affected images by *salt and pepper* and *Gaussian noise* in a visible form, respectively. It can be seen in Table 10 and Figure 15 that maximum information can be retrieved, which is a good indication of the scheme's performance.

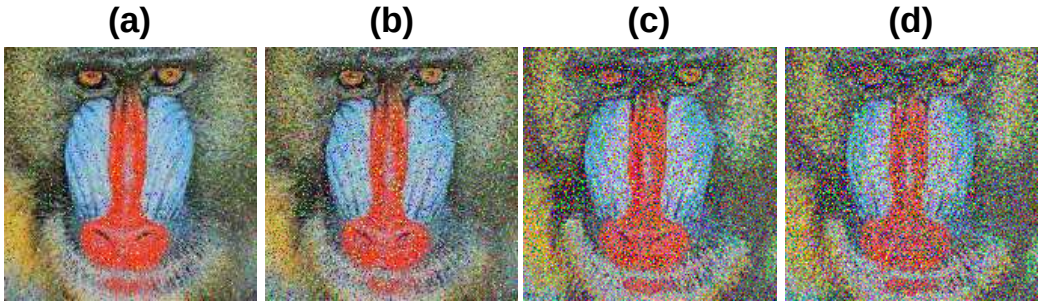

Figure 14. Resistance against *salt and pepper* on the image in Figure 2d: (**a**–**d**) images obtained by salt and pepper noise with levels of intensity 0.01, 0.02, 0.10, and 0.20, respectively.

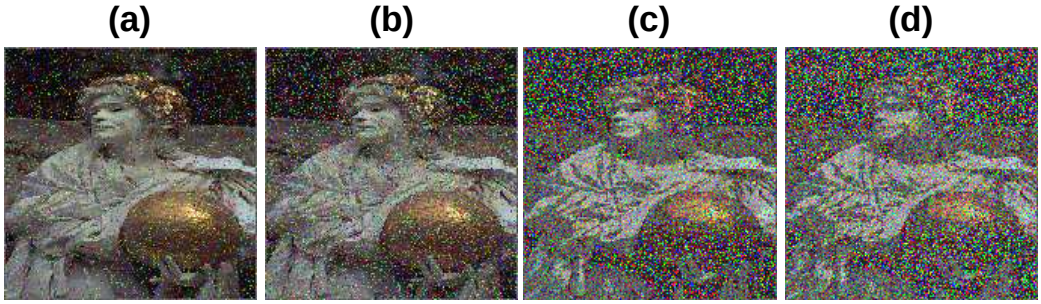

Figure 15. Resistance against *Gaussian noise* on the image in Figure 2f: (**a**–**d**) images obtained by Gaussian noise with mean = 0 and variance of 0.001, 0.002, 0.01, and 0.02, respectively.

7.9. Occlusion Attack

The durability of the system was checked against data loss through malicious destruction or deliberate attempts to damage image integrity. Occlusion attack analysis checks the recovery rate of damaged data. Thus, the encrypted baboon.jpeg image was subjected to different portions of data loss to check the data recovery rate . Figures 16a–d show the cropped images, and Figures 16e–h show the recovered images used to check the data integrity. From the recovered images, it can be seen they are visually acceptable.

The quality measures for checking the recovery rate of the affected images are provided in Table 10 and Figure 17. The results indicate that the images can be visualized, and are able to be successfully recovered against such attacks.

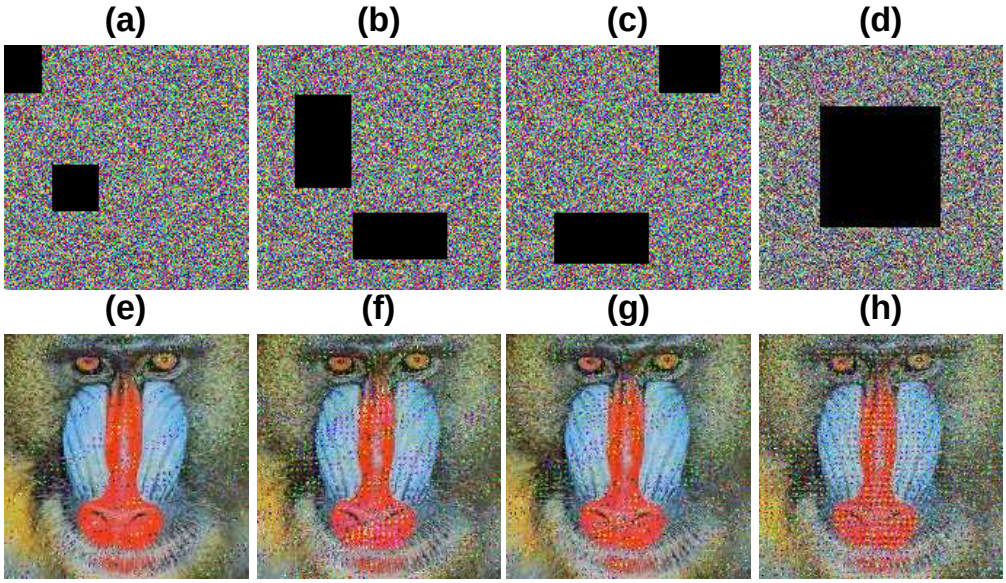

Figure 16. Occlusion attacks: (**a**) 10% occluded image, (**b**) 20% occluded image, (**c**) 25% occluded image, (**d**) 50% occluded image, (**e**–**h**) show the corresponding decrypted images.

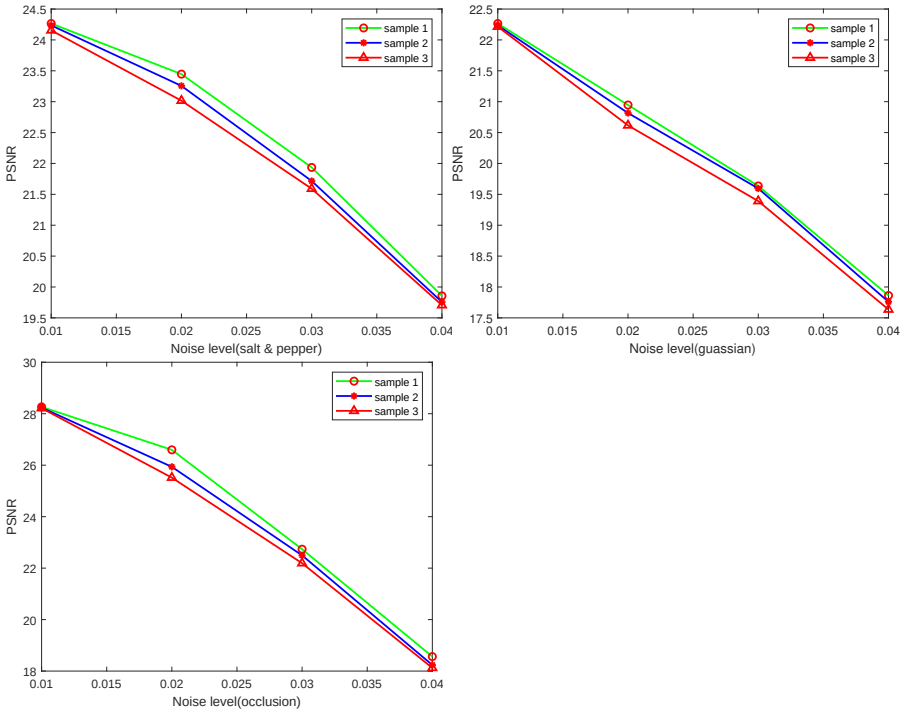

Figure 17. PSNR results of affected decrypted images.

Table 10. Quality measure of affected decrypted images.

Attacks	Image	PSNR	SSIM
Salt & pepper			
Intensity = 0.01	Baboon	24.2459	0.8756
Intensity = 0.02	–	21.2134	0.7245
Intensity = 0.01	Lady	22.5689	0.7423
Intensity = 0.02	–	17.6542	0.6359
Gaussian			
Variance = 0.001	Baboon	17.1245	0.6235
Variance = 0.002	–	15.5478	0.5932
Variance = 0.001	Lady	14.5687	0.4851
Variance = 0.002	–	12.5645	0.4315
Occlusion attack			
Occlude = 9%	Lena	28.1214	0.8932
Occlude = 20%	–	22.2547	0.7532
Occlude = 18%	–	23.3265	0.7589
Occlude = 25%	–	18.6549	0.6489

8. Conclusions

In the present paper, a serious loophole in the grayscale image encryption scheme proposed in [7] based on ECC and a Hill cipher is highlighted. The performed analysis demonstrates that the existing scheme is vulnerable and can be collapsed by a brute force attack. The competence of the scheme is in its 32-bit key length, which can be hacked using contemporary technology. To circumvent these limitations, a modified and improved version of the scheme is proposed using the classical affine Hill cipher in combination with ECC and a chaotic map for color images. The numerical and statistical results presented in Tables 5–9, the uniformity of the histogram in Figure 9, and the uniform distribution of the adjacent pixels in Figure 12 in the cipher images are enough to infer the reliability of the newly proposed method. Nevertheless, the present article lays the foundations for future work on mapping the pixel values onto $\mathbb{E}_q(a, b)$ to remove the maximum use limitation of ECDLP, and the scheme could potentially be optimized for text encryption.

Author Contributions: Conceptualization, P.N.L. and D.S.; data curation, P.N.L., D.S. and V.S.; methodology, P.N.L., V.S. and D.C.M.; formal analysis, N.K. and U.H.M.; investigation, P.N.L. and D.S.; resources, P.N.L., D.S. and U.H.M.; visualization, D.S., V.S. and D.C.M.; supervision, D.S. and N.K.; validation, P.N.L., D.S., V.S., D.C.M., U.H.M. and N.K.; writing—original draft preparation, P.N.L., D.S., V.S. and N.K.; writing—review and editing, D.S., V.S., N.K. and U.H.M.; project administration, V.S., D.C.M. and N.K.; funding acquisition, V.S. All authors have read and agreed to the published version of the manuscript.

Funding: This paper was supported by the national project of the Slovakian Ministry of Education: KEGA 013TTU-4/2021 "Interactive animation and simulation models for deep learning".

Data Availability Statement: Not applicable.

Acknowledgments: The second author is thankful to Central University of Punjab for providing the research seed money grant No: CUPB/Acad./2022/1194.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Koul, N.; Kumar, N.; Sayeed, A.; Verma, C.; Raboaca, M.S. Data Exchange Techniques for Internet of Robotic Things: Recent Developments. *IEEE Access* **2022**, *10*, 102087–102106. [CrossRef]
2. Hankerson; Menezes, A.J.; Vanstone, S.A. *Guide to Elliptic Curve Cryptography*, 2004 ed.; Springer Professional Computing; Springer: New York, NY, USA, 2004.

3. Gura, N.; Patel, A.; Wander, A.; Eberle, H.; Shantz, S.C. Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. In *International Workshop on Cryptographic Hardware and Embedded Systems, Proceedings of the Cryptographic Hardware and Embedded Systems-CHES 2004, Cambridge, MA, USA, 11–13 August 2004*; Joye, M., Quisquater, J.J., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 119–132.
4. Malan, D.; Welsh, M.; Smith, M. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. In Proceedings of the 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, IEEE SECON 2004, Santa Clara, CA, USA, 4–7 October 2004; pp. 71–80. [CrossRef]
5. Li, L.; Abd El-Latif, A.A.; Niu, X. Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images. *Signal Process.* **2012**, *92*, 1069–1078. [CrossRef]
6. Paar, C.; Pelzl, J. *Understanding Cryptography*, 2010 ed.; Springer: Berlin, Germany, 2014.
7. Dawahdeh, Z.E.; Yaakob, S.N.; Razif bin Othman, R. A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. *J. King Saud Univ.-Comput. Inf. Sci.* **2018**, *30*, 349–355. [CrossRef]
8. Hayat, U.; Ullah, I.; Azam, N.A.; Azhar, S. A Novel Image Encryption Scheme Based on Elliptic Curves over Finite Rings. *Entropy* **2022**, *24*, 571. [CrossRef]
9. Tawalbeh, L.; Mowafi, M.; Aljoby, W. Use of elliptic curve cryptography for multimedia encryption. *IET Inf. Secur.* **2013**, *7*, 67–74. [CrossRef]
10. Abd El-Latif, A.A.; Niu, X. A hybrid chaotic system and cyclic elliptic curve for image encryption. *AEU-Int. J. Electron. Commun.* **2013**, *67*, 136–143. [CrossRef]
11. Obaid, Z.K.; Saffar, N.F.H.A. Image encryption based on elliptic curve cryptosystem. *Int. J. Electr. Comput. Eng.* **2021**, *11*, 1293–1302. [CrossRef]
12. Singh, L.D.; Singh, K.M. Image Encryption using Elliptic Curve Cryptography. *Procedia Comput. Sci.* **2015**, *54*, 472–481. [CrossRef]
13. Kumar, M.; Iqbal, A.; Kumar, P. A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. *Signal Process.* **2016**, *125*, 187–202. [CrossRef]
14. Khoirom, M.S.; Laiphrakpam, D.S.; Themrichon, T. Cryptanalysis of multimedia encryption using elliptic curve cryptography. *Optik* **2018**, *168*, 370–375. [CrossRef]
15. Liu, H.; Liu, Y. Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve. *Opt. Laser Technol.* **2014**, *56*, 15–19. [CrossRef]
16. Mir, U.; Singh, D.; Mishra, D.; Lone, P. Multilayer Security of RGB Image in Discrete Hartley Domain. *Appl. Appl. Math. Int. J. (AAM)* **2020**, *15*, 1213–1229.
17. Mir, U.H.; Singh, D.; Lone, P.N. Color image encryption using RSA cryptosystem with a chaotic map in Hartley domain. *Inf. Secur. J. A Glob. Perspect.* **2022**, *31*, 49–63. [CrossRef]
18. Lone, P.N.; Singh, D.; Mir, U.H. Image Encryption Using DNA Coding and Three-Dimensional Chaotic Systems. *Multimed. Tools Appl.* **2022**, *81*, 5669–5693. [CrossRef]
19. Lone, P.N.; Singh, D. Application of algebra and chaos theory in security of color images. *Optik* **2020**, *218*, 165155. [CrossRef]
20. Sabir, S.; Guleria, V. Multi-layer color image encryption using random matrix affine cipher, RP2DFrHT and 2D Arnold map. *Multimed. Tools Appl.* **2021**, *80*, 27829–27853. [CrossRef]
21. Liu, H.; Zhu, Z.; Jiang, H.; Wang, B. A Novel Image Encryption Algorithm Based on Improved 3D Chaotic Cat Map. In Proceedings of the 2008 The 9th International Conference for Young Computer Scientists, Zhangjiajie, China, 18–21 November 2008; pp. 3016–3021. [CrossRef]
22. Joshi, A.B.; Kumar, D.; Gaffar, A.; Mishra, D. Triple color image encryption based on 2D multiple parameter fractional discrete Fourier transform and 3D Arnold transform. *Opt. Lasers Eng.* **2020**, *133*, 106139. [CrossRef]
23. Acharya, B.; Rath, G.; Patra, S.; Panigrahy, S.K. Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm. *Int. J. Secur.* **2007**, *1*, 14–21.
24. Alvarez, G.; Li, S. Some Basic Cryptographic Requirements for Chaos-based Cryptosystems. *Int. J. Bifurc. Chaos* **2006**, *16*, 2129–2151. [CrossRef]
25. Schneier, B. *Applied Cryptography*, 20th ed.; John Wiley & Sons: Nashville, TN, USA, 2015.
26. Kumar, S.; Paar, C.; Pelzl, J.; Pfeiffer, G.; Schimmler, M. Breaking Ciphers with COPACOBANA—A Cost-Optimized Parallel Code Breaker. In *International Workshop on Cryptographic Hardware and Embedded Systems , Proceedings of the Cryptographic Hardware and Embedded Systems-CHES 2006, Yokohama, Japan, 10–13 October 2006*; Goubin, L., Matsui, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 101–118.
27. Levine, J. Some Applications of High-Speed Computers to the Case n = 2 of Algebraic Cryptography. *Math. Comput.* **1961**, *15*, 254–260.
28. Lone, P.N.; Singh, D.; Mir, U.H. A novel image encryption using random matrix affine cipher and the chaotic maps. *J. Mod. Opt.* **2021**, *68*, 507–521. [CrossRef]