Concealed Chosen Plaintext Attack on Multiple S-boxes Based Image Encryption

Ahmed Rabea[1,*], Mohamed G. Abdelfattah[2], Abeer T. Khalil [3], Ali E. Takieldeen [4]

[1, 2, 3] Department of Electronics and Communications Engineering, Faculty of Engineering, Mansoura University, Mansoura, Egypt

[4]IEEE Senıor Member, Faculty of Artificial Intelligence, Delta University for Science and Technology, Gamasa 35712, Mansoura, Egypt

Emails: rabeaahmed701@std.mans.edu.eg; eng.mo.gamal@mans.edu.eg
abeer.twakol@mans.edu.eg; a_takieldeen@yahoo.com

Abstract

Chosen plaintext attacks (CPA) pose a significant security risk to encryption algorithms. However, it can be difficult to perform such an attack without direct access to the encryption process. This paper introduces a new cryptoanalysis method that uses hidden CPA to analyze image encryption schemes based on substitution boxes (S-boxes) Unlike traditional CPA methods, the proposed algorithm does not require that they can directly into the encryption process. Instead, a hidden attack vector is embedded in the natural host image to reduce the risk of attack detection. By asking the owner of the encryption algorithm to encrypt this encryption image and provide a cipher image, the input vector can be compared with its encrypted counterpart This can have an effective S-box and break encryption the algorithm, which does not interact directly with the encryption process. Experimental results demonstrate that the proposed method can completely recover cipher images in cascading S-box encryption schemes, regardless of the number of S-boxes used. Additionally, it conceals the CPA vector within the host image imperceptibly, achieving a high PSNR of 49.47 dB, indicating minimal visual distortion. Furthermore, our CPA significantly outperforms existing techniques in speed, recovering a 256×256 grayscale image in just 1.2 seconds. This method provides a simple yet effective cryptanalysis tool to evaluate the security of such image encryption schemes against CPAs.

Keywords: Cryptanalysis attacks; Substitution-boxes (S-boxes); Image encryption; Chosen plaintext attack (CPA).

1. Introduction

Information security has become a major concern in today's digital age. With the increasing use of digital images in a variety of applications, security during storage and transmission has become a major challenge. Image encryption emerges as an important component of information security, as it provides a means of protecting digital images from unauthorized access and modification but also from image encryption most methods meet safety-performance issues, emphasizing the need for comparison to determine the most appropriate method for a given application [1] appears in situations such as photo albums, medical imaging systems, military photo communications, and private video conferencing [2,3] but the security of encryption schemes against cryptanalysis attacks is a major concern.

Cryptanalysis plays an essential role in safeguarding digital data and maintaining confidentiality. It involves scrutinizing mathematical techniques used for encryption schemes to determine their security and vulnerabilities. Cryptographic algorithms and protocols are closely studied and sometimes broken through

Doi : https://doi.org/10.54216/JCIM.140108
Received: March 02, 2024 Revised: May 22, 2024 Accepted: June 11, 2024

attacks to ensure data remains protected from unauthorized access [4,5]. Without this process, it is impossible to determine whether an encryption scheme can withstand attacks. Cryptanalysis helps researchers overcome vulnerabilities by enhancing existing cryptographic processes or developing more secure ones [6,7]. This ongoing pursuit of secure encryption methods has led to a recent surge in proposals for enhanced algorithms [28-30]. One approach to image encryption relies on substitution-permutation networks (SPNs) that use S-boxes to substitute pixel values and permutation to shuffle encrypted pixels. However, recent research has shown that S-box-only image ciphers are vulnerable to chosen plaintext attacks (CPAs). In a CPA, the attacker selects plaintext and obtains corresponding cipher text from the encryption process. Many cryptanalysis algorithms relying on CPA require accessing the encryption process, making them challenging to execute. However, recent research has shown CPA can break image encryption algorithms if the attacker can access the encryption process in most cases [8, 9]. Therefore, further research on cryptanalysis and developing new and improved encryption algorithms are needed to ensure safely storing and transmitting digital images.

Symmetric- key encryption algorithms rely heavily on S-boxes as important nonlinear elements [10,11] . The addition of an S-box ensures that the nonlinear information undergoes a nonlinear transformation with each round of the encryption algorithm, thereby introducing confusion, making it difficult for attackers to extract key information in accuracy Researchers enhance the security of cryptographic techniques Nonlinearity, differential uniformity, strict As a result, image ciphers based on substitution have increasingly adopted S-boxes as a mainstream technique in recent years [12].

Several research studies have been conducted in recent years to investigate the security of image encryption algorithms that use S-boxes [13–17]. In their study, Zhang and Xiao [13] performed cryptanalysis on image ciphers that solely rely on S-boxes. They proposed four ideas for improving the design of a secure cryptosystem based on S-boxes after dis- covering vulnerabilities in these ciphers. Similarly, Zhang et al. [14] analyzed an image encryption algorithm that.used a hyper-chaotic system and a dynamic S-box. Their study revealed potential security issues as they found vulnerabilities to CPAs and also found vulnerabilities against differential cryptanalysis of dynamic S-box Using a unique chaos-based S-box to determine the security of an image encryption algorithm Zhu et al. [15] performed a latent analysis and found some weaknesses. The researchers found that the algorithm is sensitive to CPAs, while the S-box itself is not protected against differ entail cryptanalysis In another study, Liu et al. [16], discussed the weaknesses of schemes for S-Boxes, especially those resulting from fixed points and turning points. To overcome these issues, an enhanced coupling quadratic map method was introduced to design a robust and secure S-Box system. Munir and so on. [17] presented a review of the vulnerabilities found in encryption algorithms that rely heavily on S-boxes. They confirmed that systems that rely solely on S-boxes are susceptible to CPA and chosen-ciphertext attacks (CCAs), making them easier to break in. The researchers performed and proposed cryptanalysis using these attack techniques development to address the findings. Rizk-Allah et. al. [25] introduced a novel optimization algorithm specifically designed for efficient key retrieval in S-AES cryptanalysis. Leveraging a known-plaintext attack with minimal data requirements, it achieves significant accuracy improvements (>80%) compared to traditional methods. Xie and Tian [26] evaluated the security of AES-like ciphers against mixture differential cryptanalysis. They proposed a new structure called a boomerang structure and illustrated that a differential distinguisher of a boomerang structure just corresponds to a mixture differential distinguisher for AES-like ciphers. Jeong et. al. [27] performed a comprehensive neural cryptanalysis of five block ciphers - DES, SDES, AES, SAES, and SPECK. The analysis investigates the ciphers' vulnerabilities against three different attacks: Encryption Emulation (EE), Plaintext Recovery (PR), and Key Recovery (KR) attacks, as well as Ciphertext Classification (CC) attacks. It is important to acknowledge that direct access to encryption algorithms was required to perform these analyses. In conclusion, these works highlight the importance of careful design and implementation of S-box-based image encryption algorithms to guarantee security.

In this paper, A cryptanalysis algorithm is proposed that conceals the chosen plaintext vector in a meaningful host image without any visual degradation, thus reducing the likelihood of the encryption owner suspecting a CPA. In this paper, A cryptanalysis algorithm is presented that aims to attack a multiple cascaded S-box-based image encryption algorithm. The proposed cryptanalysis algorithm effectively hides the CPA vector in the host image, without any optical degradation. This approach reduces the likelihood that the encryption owner will suspect CPA. By inserting CPA vectors into the host image, a misleading CPA image that looks normal and logical is created. This allows the attacker to trick authorized users into storing this altered image and restore the CPA as an encrypted image. Once segmented, the information from the CPA cipher image can be extracted to create a CPA lookup table. This gives the attacker with the CPA gateway the ability to compromise other encrypted images with the same encryption scheme. To the best of our knowledge, this is the first work that proposes a cryptanalysis algorithm that uses the hidden

Doi : https://doi.org/10.54216/JCIM.140108
Received: March 02, 2024 Revised: May 22, 2024 Accepted: June 11, 2024

CPA method for multiple image storage based on S-box Besides, our method is independent from the configuration of the number of cascaded S-boxes used in the encryption. is about many things.

The remainder of the paper is organized as follows: Section 2 details the encryption model under study. Section 3 presents the proposed cryptanalysis algorithm. Section 4 evaluates the performance of the proposed cryptanalysis algorithm. Finally, Section 5 provides concluding remarks.

2. Encryption Model Under Study

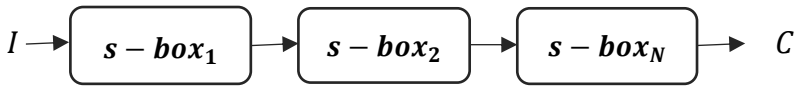


Figure 1: Understudy Encryption Model

This section introduces the image encryption model that will underpin our cryptoanalysis. Our research focuses on an improved image encryption method that uses several cascade boxes to enhance security, as in Fig 1. S-boxes are used to replace data blocks with targets, and in a mining manner effectively applied to the original image data between the form of the S-box without the same knowledge or knowledge of the associated key, it will be difficult to manipulate. Unlike traditional approaches to cryptanalysis [13–17], which mainly target a one-dimensional S-box-based image encryption scheme, our model is extensible and makes this concept inclusive of each by adding several steps that take place in these cryptographic aspects The encryption model consists of the following step:

1. Each pixel in the plain image is sequentially processed by each of the S-boxes in a cascading manner.
2. The output from one S-box serves as the input for the next stage, continuing this process until the final output, which is the cipher image, is generated.

The original image can be recovered by applying the inverse of the S-box series used for encryption in reverse order. This approach is deemed more secure compared to utilizing a single S-box stage because its complexity poses challenges for attackers attempting to analyze the process. Through our cryptanalysis, The effectiveness of this encryption model is assessed and identify the potential vulnerabilities that could be exploited by attackers.

3. Proposed Cryptanalysis Algorithm

In this section, a hidden search algorithm is proposed to attack an image storage system using multiple cascade boxes described in Section 2. The algorithm is designed on the assumption that the attacker does not know which S-boxes are used to control the type or number of users Encryption policy. Its purpose is to get a CPA lookup table with two rows. The first row is the CPA vector labeled CV and the second row represents S(CV), which shows the corresponding output from the effective S-box for each input value of In the CV row.

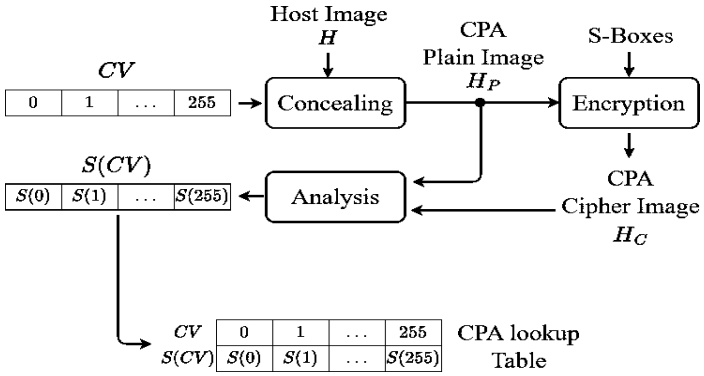


Figure 2: Proposed Cryptanalysis Algorithm

The steps of this cryptanalysis algorithm are illustrated in Fig. 2 and can be described as follows:

Doi : https://doi.org/10.54216/JCIM.140108
Received: March 02, 2024 Revised: May 22, 2024 Accepted: June 11, 2024

1. Prepare a CPA vector CV consisting of integer numbers from 0 to 255, representing all possible intensity levels in an 8-bit grayscale image:

$$CV = [0, 1, \ldots\ldots\ldots\ldots, 255] \quad (1)$$

2. Select a normal host image H to imperceptibly conceal CV inside, ensuring that the visual quality of the host image.
3. To conceal the CPA vector CV within the host image H, each pixel is compared in H with every intensity level present in CV. If any levels are missing from H, they are embedded into the image without significantly altering its visual appearance. This is achieved by selecting the pixel with the least absolute difference to the corresponding missing intensity level and replacing it with that intensity level. The resulting image is the CPA plain image H_P, which contains all intensity levels in CV and appears normal. The process can be mathematically represented by the equation:

$$H_P(x,y) = \begin{cases} H(x,y) & \text{if } H(x,y) \in CV \\ \min_{c \in CV} |H(x,y) - c|, & \text{otherwise} \end{cases} \quad (2)$$

where $H_P(x, y)$ is the pixel value of the CPA plain image at location (x, y) and $H(x, y)$ is the pixel value of the host image at location (x, y). The resulting H_P image can be given to the owner without raising suspicion.

4. The attacker tricks the owner of the encryption algorithm by presenting H_P as a normal image that needs to be encrypted. The owner encrypts the image and returns the resulting CPA cipher image H_C to the attacker.
5. The intensity levels in H_P and H_C are compared to obtain the second row of the CPA table S (CV).
6. The attacker can use the CPA table to attack any cipher image x generated by the same encryption algorithm. This is done by replacing each pixel in C with the corresponding value in the CPA table. This method is independent of the number of cascaded S-boxes used in the encryption process. Consequently, once the attacker gains access to the CPA table, the encryption algorithm breaks down completely.

4. Numerical Results

Numerical simulations are performed to demonstrate the feasibility and efficiency of the proposed cryptanalysis algorithm. Through these simulations, It will be demonstrated that The algorithm is capable of performing crypt analysis on several cascaded S-box-based encryption algorithms using any or any number of boxes. In our simulations, the three different are used S-boxes: (i) the AES S-box shown in Table 1, (ii) the Razaq S-box [18] shown in Table 2, and (iii) the Gupta S-box[19] shown in Table 3. a 256×256 gray scale "Trucks" image is utilized, shown in Fig. 3 (a), as the host image H for the cryptanalysis algorithm. Additionally, a 256×256 grayscale "Sailboat" image is used, shown in Fig. 3 (b), as the secret plain image owned by the encryption algorithm owner that needs to be secured.

(a) (b)

Figure 3: (a) Host image; (b) Secret plain image.

4.1 Concealing Process

The CPA vector CV should be concealed in the host image H imperceptibly so that the resulting CPA image H_P does not arouse any suspicion from the encryption algorithm owner.

Doi : https://doi.org/10.54216/JCIM.140108
Received: March 02, 2024 Revised: May 22, 2024 Accepted: June 11, 2024

(a) (b)

Figure 4: (a) Host image; (b) CPA image

Table 1: AES S-Box

63	7C	77	7B	F2	6B	6F	C9	30	1	67	2B	FE	D7	AB	76
CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
4	C7	23	C3	18	96	5	9A	7	12	80	E2	EB	27	B2	75
9	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
53	D1	0	ED	20	FC	B1	5B	6A	CB	BE	37	4A	4C	58	CF
D0	EF	AA	FB	43	4D	33	85	49	F9	2	7F	50	3C	9F	A8
51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
CD	0C	13	EC	5F	97	68	17	C4	A7	7E	3D	64	5D	19	73
60	81	79	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
E0	32	3A	0A	49	6	24	5C	C2	D3	A6	62	41	91	95	E4
77	E0	37	69	6D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	8
BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
70	3E	B5	66	48	3	F6	0E	61	35	57	B9	86	C1	1D	9E
E1	F8	98	A1	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Table 2: Razaq S-Box

24	D9	62	0	21	CD	9F	5E	40	DC	C3	33	71	57	91	35
51	2C	42	34	3F	20	28	47	3C	55	63	0B	39	65	9A	37
EE	74	9	25	38	2F	83	52	56	E9	18	11	E1	5B	8A	D8
9C	EC	85	9D	F8	B3	5C	99	E3	B6	72	5	BF	94	84	E7
14	4	FE	13	F7	0F	BC	1	CB	FF	F6	1B	54	7E	EA	3A
19	C0	A9	3B	C7	64	36	B8	FD	D2	DA	CF	78	32	10	30
89	6E	A5	CA	0C	F2	93	A7	A4	B5	A2	7D	B9	92	58	73
67	5A	C2	0A	BE	D3	C4	15	B2	F4	4C	7C	BA	A0	A6	FC
DB	EB	76	DF	98	E8	BB	F9	4D	8F	31	ED	D0	1E	7A	4F
45	EF	7F	49	D7	AB	66	27	79	80	C9	FA	2D	1A	B0	61
59	DD	8C	2E	8E	22	69	F3	E4	D4	6C	26	F1	CE	C5	4E
16	F0	70	C8	82	2	2A	AC	4B	29	1C	C5	A1	6A	D6	AA
3	77	BD	8D	90	0D	6B	6D	43	5D	AE	44	75	E0	3D	95
1D	4A	7	86	F5	AF	88	E6	3E	60	17	41	0E	96	D5	CC
50	81	68	97	DE	6	E2	FB	48	2B	46	5F	B1	B4	7B	12
A3	E5	9E	23	87	8B	B7	A8	6F	8	AD	D1	C6	53	1F	9B

In our experiment, CV inside the host "Trucks" image is concealed, shown in Fig. 4 (a), and the resulting CPA plain image is shown in Fig. 4(b). The quality of the CPA plain image remains intact with no noticeable degradation, making it visually indistinguishable from the original host image. This indicates that our approach effectively conceals and embeds the CPA vector into the host image. The quality of the CPA image is quantified using the peak signal-to-noise ratio (PSNR):

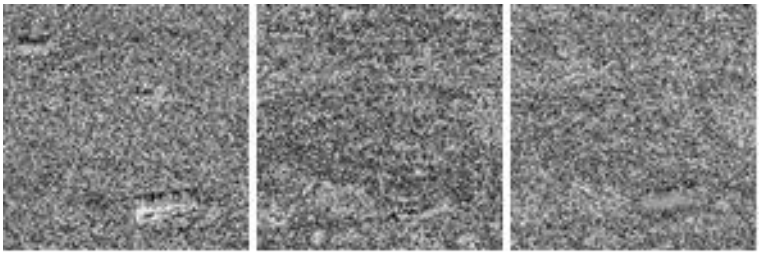
$$\text{PSNR} = 10\log_{10}\left(\frac{\text{MAX}_I^{\,2}}{\frac{1}{M\,N}\sum_{i=0}^{\text{M}-1}\sum_{\text{j}=0}^{\text{N}-1}\left(\text{H}(i,\text{j}) - H_P(i,\text{j})\right)^2}\right). \quad (3)$$

Doi : https://doi.org/10.54216/JCIM.140108
Received: March 02, 2024 Revised: May 22, 2024 Accepted: June 11, 2024

Here, MAX_H is the maximum possible pixel value of the host image H, which is 255 for an 8-bit grayscale image, M and N are the height and width of the image in pixels, $H(i,j)$ and $H_P(i,j)$ represent the pixel values of the host and the CPA images at position (i,j), respectively. Mathematically, the PSNR between H and H_P is 49.47 dB, confirming negligible visual differences between the two images.

4.2 Chosen Plaintext Attack

To test the effectiveness of the cryptanalysis algorithm to crack the understudy encryption algorithm, regardless of the number and type of S-boxes used, the attack is performed under three different scenarios These cases include using S -one box (AES S-box) will be used Two S-boxes (AES S-box and Razaq S-box), and three cascaded S-boxes (AES S-box, Razaq S-box, and Gupta S-box). If the encryption algorithm is successfully broken in these scenarios, it can be inferred that the cryptanalysis algorithm is effective. Furthermore, this indicates that the cryptanalysis algorithm is capable of breaking the encryption algorithm even when more than three S-boxes are employed.



(a) (b) (c)

Figure 5: CPA Cipher Images Using (a) Single S-Box; (b) Two S-Boxes; (c) Three S-Boxes.

Table 3: Gupta S-box [19]

15	0E	58	9C	3	34	62	9B	F7	95	A5	AE	C2	43	C9	F0
89	1A	DA	6D	24	BA	7	74	56	4B	CB	93	CD	AD	6C	72
5E	42	39	6F	C5	E4	5B	1	68	0B	12	A7	A2	5F	27	41
1E	9D	82	0	D0	2A	F2	B0	B3	EF	1B	7B	55	83	AC	BB
88	7E	FF	17	75	E8	78	5D	4F	4E	FB	3A	59	E9	D5	B8
C4	D1	81	F6	86	66	BD	3B	47	2D	99	8F	6E	7F	A3	F4
20	7A	79	92	1D	37	1C	D6	65	C6	84	B5	2E	A9	0C	60
B9	19	77	8A	94	0D	CA	ED	0F	71	57	6	63	D7	45	F3
E7	BE	4A	69	5	64	F8	25	26	E5	4D	18	76	F1	4C	4
35	14	46	30	2	B1	DD	E2	13	B6	8	FC	36	1F	33	9A
85	31	C0	21	D2	61	2C	B7	70	DF	8E	10	D9	22	CE	A6
87	32	8D	D8	EE	FD	3D	EB	A0	11	73	E6	29	CF	EC	6B
C1	7D	DB	51	54	3F	28	9	FE	3E	16	BF	EA	9E	2B	A1
7C	B2	6A	F5	23	96	DE	0A	D3	38	C3	C7	C8	D4	2F	67
3C	48	DC	50	52	8B	E3	A8	5A	5C	B4	90	97	E1	53	49
F9	80	40	AA	E0	AF	AB	FA	BC	8C	98	CC	44	9F	A4	91

In our simulation, the attacker requests the encryption algorithm owner to encrypt the CPA image H_P shown in Fig. 4 (b) that appears normal and meaningful. However, it contains the hidden CPA vector CV. The CPA image is encrypted using the three scenarios: utilizing one S-box (AES S-box), cascading two S-boxes (AES S-box and Razaq S-box), and cascading three S-boxes (AES S-box, Razaq S-box, and Gupta S-box). The resulting cipher images H_C for each scenario are presented in Fig. 5 (b-d) respectively. Subsequently, the owner sends the CPA cipher images to the attacker, who analyzes them to construct the CPA lookup tables. For the three scenarios, the constructed CPA tables are depicted in Table 4, respectively.

With these constructed CPA tables, it is possible to successfully attack any cipher image generated from the same encryption algorithm and successfully retrieve the secret plain image. To verify this claim, an experiment is conducted where the encryption algorithm is applied to the Sailboat image depicted in Fig. 3 (b), using each of the three mentioned scenarios. The original image is attempted to be recovered by using the CPA tables.

Doi : https://doi.org/10.54216/JCIM.140108
Received: March 02, 2024 Revised: May 22, 2024 Accepted: June 11, 2024

Table 4: Chosen plaintext attack (CPA) lookup tables.

CV	0	1	2	3	4	5	….	252	253	254	255
$\mathcal{S}_1$(CV)	99	124	119	123	242	107	….	176	84	187	22
$\mathcal{S}_2$(CV)	202	186	21	124	158	125	….	22	199	197	40
$\mathcal{S}_3$(CV)	22	115	186	99	51	215	….	7	9	63	104

The original Sailboat image, shown in Fig. 6 (a), is encrypted using the three scenarios. The resulting cipher images are shown as follows: Cipher 1, obtained after applying one S-box (AES S-box) is shown in Fig. 6 (b); Cipher 2, obtained after applying the two cascaded S-boxes (AES S-box and Razaq S-box) is shown in Fig. 6 (c); and Cipher 3, obtained after applying the three cascaded S-boxes (AES S- box, Razaq S-box, and Gupta S-box) is shown in Fig. 6 (d). Using the CPA tables, depicted in Table 4, the cipher images shown in Fig. 6 (b)-(d) are attacked individually under each of the three scenarios. Remarkably, the retrieved image is identical in all three cases, as displayed in Fig. 6 (e), and visually indistinguishable from the original plain image in Fig. 6 (a). This confirms that the original plain image is successfully retrieved with an infinite PSNR.

The correlation between adjacent pixels in the original, cipher, and recovered images can be calculated using:

$$r_{xy} = \frac{E\{(x-m_x)(y-m_y)\}}{S_x S_y}, \tag{4}$$

where $E\{\cdot\}$ represents the mathematical expectation, m denotes mean value, and S symbolizes standard deviation.

Table 5: correlation between adjacent pixels in the original, cipher, and recovered images in horizontal, vertical, and diagonal directions.

Image	Correlation direction		
	Horizontal	Vertical	Diagonal
Original	0.9593	0.9589	0.9314
Cipher1	0.1133	0.1120	0.0960
Cipher2	0.1180	0.1145	0.1008
Cipher3	0.0848	0.0748	0.0662
Recovered	0.9593	0.9589	0.9314

This correlation measures the correlation value between adjacent pixels *x and y* in the horizontal, vertical, and horizontal directions. Correlation coefficient values are calculated for the original, cipher and recovered images, as shown in Table 5. As expected, neighboring pixels in the original image exhibit stronger correlations in all three directions, which values one when the correlation coefficient for the cipher images is negligible close to zero. Moreover, the correlation coefficients of the original and recovered images are identical, indicating that the proposed attack can successfully recover the original image.

Correlation diagrams are designed to visually represent the correlation values of the original, cipher, and recovered images in the horizontal, vertical, and distal directions with this correlation diagram species are shown in the second, third and fourth columns of Fig. 6. The figures clearly show that the encryption algorithm effectively removes the correlation between pixels in all directions. Furthermore, the correlation images show that the original images are identical to the pixel distribution of the recovered images. This similarity shows that the proposed CPA succeeds in recovering the original image.

4.3 histogram Analysis

The distribution characteristics of a histogram can also be described quantitatively with the variance of a histogram, which is calculated as

$$\text{var(p)} = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}(p_i - p_j)^2, \tag{5}$$

Doi : https://doi.org/10.54216/JCIM.140108
Received: March 02, 2024 Revised: May 22, 2024 Accepted: June 11, 2024

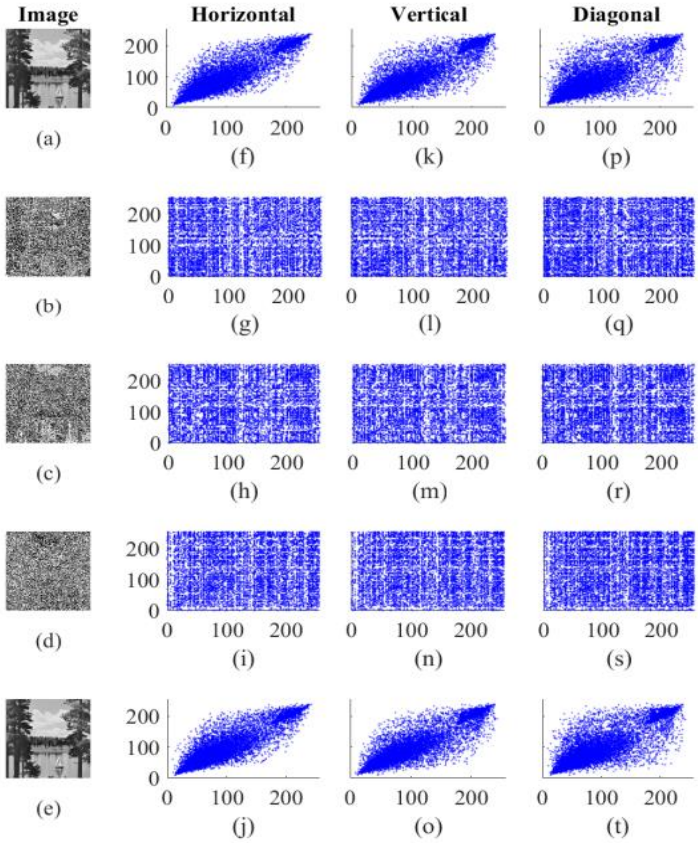


Figure 6: Adjacent pixel correlation diagrams: (a) original image, (b)-(d) cipher images after applying one, two, and three S-boxes, respectively; (e) recovered image (f)-(j) horizontal, (k)-(o) vertical, and (p)-(t) diagonal correlation of the original, cipher, and recovered images displayed in (a)-(e).

where, n is the number of gray levels of an image, and n = 256 for 8-bit gray images. Z is a vector and Z = $\{p, p_2, \ldots, p_n\}$, p_i and p_j are the numbers of pixels with gray values equal to $(i - 1)$ and $(j - 1$ respectively. The lower price of variance indicates the better uniformity of a photo. To discover the variance values of the above check pix and their cipher pictures, the variances of the histograms of the plain photographs (of size 256 × 256) and their cipher images are calculated by using Equation (5). The outcomes are listed in Table.6. Table.6 also lists the results received with the aid of the set of rules in References [20] and [21]. The average variance of 4 cipher pictures acquired with our proposed set of rules is 256.7125, which is plenty much less than that of Zhang's set of rules [20], and Wang's set of rules [21], Thus, our proposed photo encryption algorithm has higher overall performance in resisting statistical assaults.

Table 6: Variances of histograms of the test images.

Images	Plain Image	Cipher Image	Cipher Image [20]	Cipher Image [21]
Trucks	36,379.134	224.233	269.728	227.897
Sailboat	47,799.057	288.663	268.212	277.296
All-white image	16,711,681	293.038	544.233	41,725.062
All-black image	16,711,682	256.431	1396.764	43,233.187
Average	6,707,640.776	256.714	552.702	17,149.321

4.4 Time complexity analysis

The proposed cryptanalysis algorithm will then analyze the time complexity, which is mainly determined by three processes: the encryption scheme, the encryption of the CPA image, and the search through the CPA table to attack the cipher image. For an image of size M × N, the worst-case complexity for each pixel in the concealing and searching processes is 256. However, the complexity of encrypting the CPA image also depends on the number of S- box stages, denoted by s. Therefore, the upper bound for the computational complexity is O [256 M N $(s + 2)$].

Doi : https://doi.org/10.54216/JCIM.140108
Received: March 02, 2024 Revised: May 22, 2024 Accepted: June 11, 2024

To evaluate the performance of the proposed cryptanalysis algorithm, Experiments were conducted using MATLAB R2023a on a desktop PC equipped with a Core i7 processor and 32 GB RAM. The execution times for each stage of attacking different-sized images are measured and presented in Table 7. It can be observed that there is an approximately linear increase in execution time as the size of the image increases. This is because, in the worst case, the algorithm must process each pixel of the image, and the number of pixels increases linearly with the size of the image. Therefore, it is important to consider the image size when evaluating the performance of the algorithm.

Table 7: Time complexity analysis in seconds for cryptanalysis of images with different sizes.

Size	Process		
	Concealing	Encryption	Attacking
256×256	0.5781	0.195	0.953
512×512	2.891	0.234	3.0625
1024×1024	6.422	0.565	6.641

4.5 Analyzing Comparative Execution Times

The execution time of the selected plaintext attack is compared with the standard cryptanalysis scheme in Table.8. From the listed comparison, Truck images of different sizes have been taken and recovered in a shorter time compared to the attacks presented in [22] Differences of the chosen ciphertext attacks in the table is illustrated in Table.9. The comparative results verify that the performance of the proposed attack is significantly better than the attack used in reference [22].

Table 8: Comparative analysis of chosen-plaintext attack.

Image size	Proposed attack	Ref [22]
256×256	1.2	8.51
512×521	2.1	18.12

Table 9: Comparative analysis of chosen-ciphertext attack.

Image size	Proposed attack	Ref [22]
256×256	0.4	7.01
512×521	0.7	14.34

4.6 Proposed Improvement

The proposed cryptanalysis algorithm can completely crack the encryption algorithm because it relies only on S-box and has no relationship with simple image or cipher In order to improve the encryption algorithm and prevent cracking by CPA is to be set based on S-boxes and ordinary diagrams This can be done by updating the S-boxes according to the properties of the ordinary diagram itself, so that any changes diagram of the smoother will cause changes in the S-boxes as well.

Furthermore, according to Claude Shannon's theory [23], a secure encryption algorithm should contain both confusion and diffusion. While S-boxes offer only confusion in the algorithm, it is essential to also include diffusion for enhanced security. Confusion refers to the process of making the relationship between the plaintext and ciphertext as complex as possible, while diffusion refers to the process of spreading the influence of each bit of the key throughout the ciphertext. By establishing an adjacent association between the S-boxes and plain image, the encryption algorithm can achieve both confusion and diffusion, making it more secure against attacks such as CPA [24].

5. Conclusion

Additional cryptographic plaintext (CPA) attacks have been proposed in several substitution-box (S-box)-based image encryption schemes. This method embeds the CPA vector in the image of a common host to hide the attack and reduce the risk of detection. By analyzing a CPA cipher image, an attacker can create a

Doi : https://doi.org/10.54216/JCIM.140108
Received: March 02, 2024 Revised: May 22, 2024 Accepted: June 11, 2024

lookup table to compromise other cipher images created with the same encryption scheme. The experimental results showed that this method can effectively break the security of the less-studied encryption scheme and accurately recover the original image Analysis is performed on time complex analysis of a proposed algorithm of the wisdom of the also. The time complexity of the proposed algorithm is investigated, and improvements to the less-studied encryption algorithm are suggested to increase its security and make it immune to CPA and other cryptanalysis techniques.

References

[1] Huang, H.. Novel scheme for image encryption combining 2d logistic-sine-cosine map and double random-phase encoding. IEEE Access 2019;7:177988–177996.

[2] Ahmed Rabea, Mohamed Abdelfattah, Ali Takieldeen, and Abeer Khalil. "Survey Image Cryptanalysis Using a Substitution Box Based Chaotic Map." International Journal of Telecommunications 3, no. 02 (2023): 1-12.

[3] Kumari, M., Gupta, S., Sardana, P.. A survey of image encryption algorithms. 3D Research 2017;8:1–35.

[4] Kidmose, A.B., Tiessen, T.. A formal analysis of boomerang probabilities. IACR Transactions on Symmetric Cryptology 2022;:88–109.

[5] Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.. Handbook of applied cryptography. CRC press; 2018.

[6] Ramasamy, P., Ranganathan, V., Kadry, S., Damaševičius, R.Blažauskas, T.. An image encryption scheme based on block scram- bling, modified zigzag transformation and key generation using enhanced logistictent map. Entropy 2019;21(7):656.

[7] Kendhe, A.K., Agrawal, H.. A survey report on various cryptanalysis techniques. International Journal of Soft Computing and Engineering (IJSCE) 2013;3(2):287–293.

[8] Bakhshandeh, A., Eslami, Z.. An authenticated image encryption scheme based on chaotic maps and memory cellular automata. Optics and Lasers in Engineering 2013;51(6):665–673.

[9] He, H., Yuan, Y., Ye, Y., Tai, H.M., Chen, F.. Chosen plaintext attack on jpeg image encryption with adaptive key and run consistency. Journal of Visual Communication and Image Representation 2023;90:103733.

[10] Walid Souror., Mohamed Fouad, and Ali E. Takieldeen. " Hybrid- Blowfish Security Strengths Using Side Channel Countermeasures " In 2023 International Telecommunications Conference (ITC-Egypt), pp. 1-5. IEEE, 2023.

[11] Forouzan, B.A., Mukhopadhyay, D.. Cryptography and network security; vol. 12. Mc Graw Hill Education (India) Private Limited New York, NY, USA:; 2015.

[12] Abduljabbar, Z.A., Abduljaleel, I.Q., Ma, J., Al Sibahee, M.A., Nyangaresi, V.O., Honi, D.G., et al. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access 2022;10:26257–26270.

[13] Zhang, Y., Xiao, D.. Cryptanalysis of s-box-only chaotic image ciphers against chosen plaintext attack. Nonlinear Dynamics 2013;72:751–756.

[14] Zhang, X., Nie, W., Ma, Y., Tian, Q.. Cryptanalysis and improvement of an image encryption algorithm based on hyper-chaotic system and dynamic s-box. Multimedia Tools and Applications 2017;76:15641–15659.

[15] Zhu, C., Wang, G., Sun, K. Cryptanalysis, and improvement on an image encryption algorithm design using a novel chaos based s-box. Symmetry 2018;10(9):399.

[16] Liu, H., Kadir, A., Xu, C. Cryptanalysis and constructing s-box based on chaotic map and backtracking. Applied Mathematics and Computation 2020;376:125153.

[17] Munir, N., Khan, M., Shah, T., Alanazi, A.S., Hussain, I.. Cryptanalysis of nonlinear confusion component based encryption algorithm. Integration 2021;79:41–47.

[18] Razaq, A., Iqra, , Ahmad, M., Yousaf, M.A., Masood, S.. A novel finite rings based algebraic scheme of evolving secure s-boxes for images encryption. Multimedia Tools and Applications 2021;80:20191–2021.

[19] Gupta, M.D., Chauhan, R.K.. Secure image encryption scheme using 4d-hyperchaotic systems based reconfigurable pseudo-random number generator and s-box. Integration 2021;81:137–159.

[20] Zhang, Xuan-Ping, et al. "Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes." Chinese Physics B 27.8 (2018): 080701.

[21] Wang, Xiong, et al. "S-box based image encryption application using a chaotic system without equilibrium." Applied Sciences 9.4 (2019): 781.

[22] Munir, Noor, et al. "Cryptanalysis of nonlinear confusion component based encryption algorithm." Integration 79 (2021): 41-47.

Doi : https://doi.org/10.54216/JCIM.140108
Received: March 02, 2024 Revised: May 22, 2024 Accepted: June 11, 2024

[23] Bedir Yousif, Fahmi Khalifa, Ahmed Makram, and Ali Takieldeen. "A novel image encryption/decryption scheme based on integrating multiple chaotic maps." AIP Advances 10, no. 7 (2020).
[24] Walid W. Souror, Mohamed Fouad, and Ali E. Takieldeen. "Hybrid Security Enhancement of ECC with Side Channel and Sign Fault Attack Countermeasures." In 2022 International Telecommunications Conference (ITC-Egypt), pp. 1-5. IEEE, 2022.
[25] Rizk-Allah, R. M., Abdulkader, H., Elatif, S. S. A., Oliva, D., Sosa-Gómez, G., & Snášel, V. (2023). On the Cryptanalysis of a Simplified AES Using a Hybrid Binary Grey Wolf Optimization. Mathematics, 11(18), 3982.
[26] Xie, X., & Tian, T. (2023). Structural evaluation of AES-like ciphers against mixture differential cryptanalysis. Designs, Codes and Cryptography, 91(12), 3881-3899.
[27] Jeong, O., Ahmadzadeh, E., & Moon, I. (2024). Comprehensive Neural Cryptanalysis on Block Ciphers Using Different Encryption Methods.
[28] Fath Allah, M. I. (2022). Chaos Based Stego Color Image Encryption. Journal of Cybersecurity and Information Management (JCIM), 10(2).
[29] Goel, V., & Goyal, A. K. (2023). An Improved Analysis of Secured Permutation and Substitution based Image Encryption. Journal of Cybersecurity and Information Management (JCIM) Vol, 12(01), 30-40.
[30] Yasser, I., Khalil, A. T., Mohamed, M. A., & Khalifa, F. (2021). A new chaos-based approach for robust image encryption. Journal of Cybersecurity and Information Management (JCIM), 7, 51-64.

Doi : https://doi.org/10.54216/JCIM.140108
Received: March 02, 2024 Revised: May 22, 2024 Accepted: June 11, 2024