A Robust Steganographic Algorithm based on Linear Fractional Transformation and Chaotic Maps

Steganographic Algorithm based on S-Boxes

Muhammad Ramzan[1], Muhammad Fahad Khan[2]
Department of Computer Science-College of Computing and Informatics,
Saudi Electronic University, Riyadh 11673, Saudi Arabia[1]
Department of Software Engineering, Foundation University Islamabad, 44000, Pakistan[2]

***Abstract*—The fundamental objectives of a steganographic technique are to achieve both robustness and high-capacity for the hidden information. This paper proposes a steganographic algorithm that satisfies both of these objectives, based on enhanced chaotic maps. The algorithm consists of two phases. In the first phase, a cryptographic substitution box is constructed using a novel fusion technique based on logistic and sine maps. This technique overcomes existing vulnerabilities of chaotic maps, such as frail chaos, finite precision effects, dynamical degradation, and limited control parameters. In the second phase, a frequency-domain-based embedding scheme is used to transform the secret information into ciphertext by employing the substitution boxes. The statistical strength of the algorithm is assessed through several tests, including measures of homogeneity, correlation, mean squared error, information entropy, contrast, peak signal-to-noise ratio, energy, as well as evaluations of the algorithm's performance under JPEG compression and image degradation. The results of these tests demonstrate the algorithm's robustness against various attacks and provide evidence of its high-capacity for securely embedding secret information with good visual quality.**

***Keywords*—Steganography; information security; chaotic map vulnerabilities; enhanced chaotic maps; S-box Design**

I. INTRODUCTION

History has demonstrated that secret communication has always been an essential requirement in human society. As time progressed, more advanced techniques have been introduced. In the last two decades, the rapid development of digital communication systems has significantly increased the demand for secure data exchange through digital multimedia. Innovative strategies to protect confidential information from intruders have become the focus of recent research. In this regard, modern techniques of cryptography, watermarking, and steganography have gained unusual importance in the last few years [1-5]. Cryptography involves converting useful information into dummy data to protect it from unintended recipients, while watermarking is associated with protecting the data's copyright. Steganography, on the other hand, conceals confidential information into other information [6-8]. With the advent of modern computer technology, remarkable skills for surreptitious communication have been developed. Steganography involves embedding secret information in either the spatial or transform (frequency) domain. In spatial domain embedding, the LSB-substitution technique is most commonly used. However, in the transform domain, invertible transforms such as (DCT) and (DWT) are typically applied to transform the image into its frequency representation [9-11]. While both domains have advantages and disadvantages, frequency domain embedding is robust, while spatial domain offers increased capacity for hiding data. This motivates researchers to deploy a combination of both domains. The transforms DCT and DWT are frequently used in image compression applications due to their favorable features. DCT is the most widely used, requiring fewer computational resources; however, DWT is considered more efficient in quality. Many multimedia applications and algorithms in recent literature are based on the joint applications of DCT and DWT [12-15]. In our proposed method, we apply a hybrid of these transforms for improved and robust outcomes.

In the last decade, chaos has been widely used to enhance the security level of confidential communication. Chaotic systems possess prime features such as irregularity, butterfly effect and unpredictability which making them well-suited for multimedia security applications. Consequently, the study and analysis of chaos-based steganographic techniques have gained popularity in recent years. However, it has been observed that some chaos-based methods are vulnerable to statistical analysis because of the limited chaotic range of the used maps [16-20]. To overcome this issue, authors of [19] proposed a nonlinear combination of one-dimensional chaotic maps that enhances the chaotic range of the resulting system. Such systems are applied in image encryption applications, but to the best of our knowledge, they have not been applied in steganographic methods yet.

The fundamental objectives of a steganographic technique are to achieve both robustness and high-capacity for the hidden information. This paper proposes a steganographic algorithm that satisfies both of these objectives, based on enhanced chaotic maps. The algorithm consists of two phases. In the first phase, a cryptographic substitution box is constructed using a novel fusion technique based on logistic and sine maps. This technique overcomes existing vulnerabilities of chaotic maps, such as frail chaos, finite precision effects, dynamical degradation, and limited control parameters. In the second phase, a frequency-domain-based embedding scheme is used to transform the secret information into ciphertext by employing the substitution boxes. In addition, we exploit the combination of the spatial and

transform domains to achieve a significantly high capacity level for embedding secret data. Our technique uses a hybrid of DCT and DWT, and we observe that the combined effect of DCT and DWT increases robustness against several image processing attacks. The strength of the proposed method is evaluated through the most frequently used analysis techniques, and we prove that our technique produces coherent results. The use of enhanced chaotic systems in steganography has been demonstrated to be effective in various studies, highlighting the potential for further development in this field. The structure of the paper is organized as follows: Section II presents the chaotic map fusion technique. Section III describes the design of the S-box. Section IV presents a novel steganographic technique and Section V provides the security analysis and simulation results. Finally, Section VI presents the conclusions.

II. Fusion of 1-Dimension Chaotic Maps

The study of security protocols has demonstrated the extensive applications of one-dimensional chaotic maps due to their simple structure and computational convenience. In our research, we use the logistic map and the sine map to develop a stronger chaotic system for our problem. In the upcoming sections, we explored the essential features of these maps and their implementation in our research.

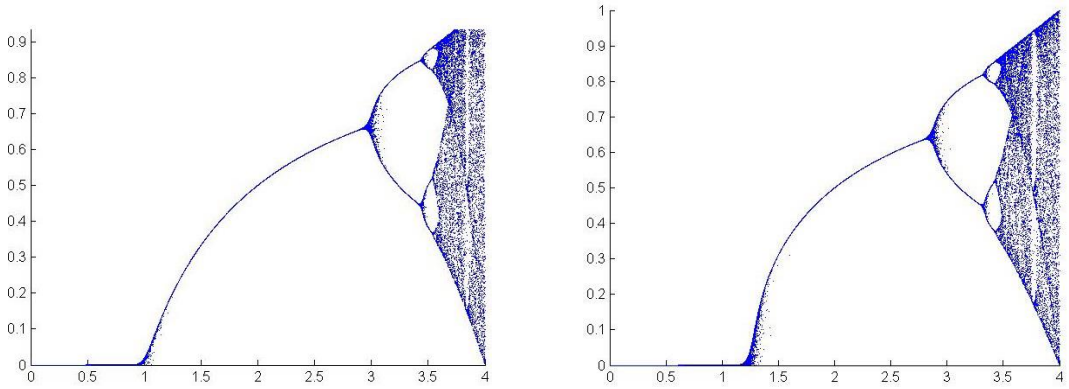
A. The Logistic Map

It is a mathematical function that has been used in various applications in information security due to its ability to generate chaotic and pseudorandom sequences. The logistic map is defined by a quadratic recurrence, which can be written as:

$$\mathcal{C}_{\mathcal{L}}(\vartheta_{\mathcal{L}}, x_i) = \vartheta_{\mathcal{L}} x_i(-x_i); \quad (1)$$

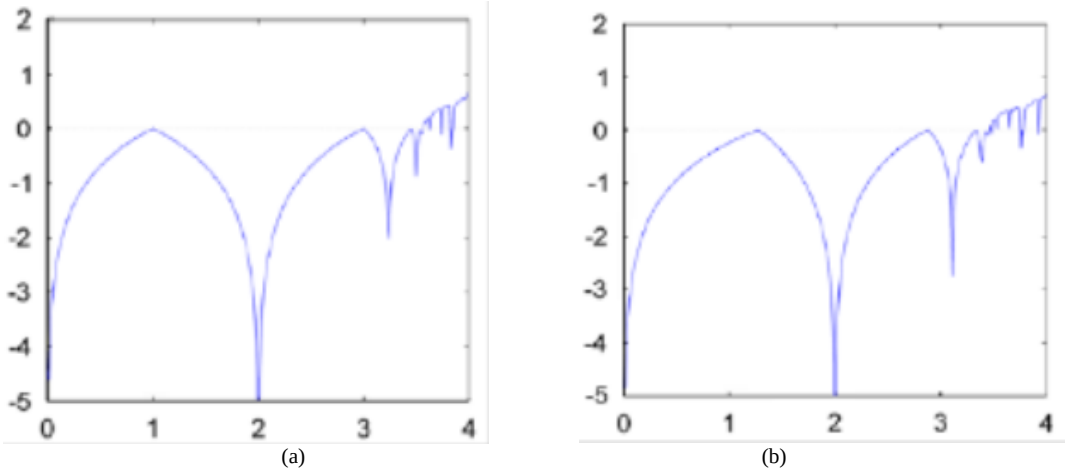
Where $\vartheta_{\mathcal{L}} \in (0, 4]$ is called the control parameter. It is also known *as a catalyst* for chaos as the behavior of the map varies when the value of parameter $\vartheta_{\mathcal{L}}$ changes. It is clear from the bifurcation diagram (as shown in Fig. 1(a)) that $\mathcal{C}_{\mathcal{L}}$ produces the chaotic effect only when $\vartheta_{\mathcal{L}} \in [3.57, 4]$. Although the Logistic map is widely used, it has been noted that its chaotic range is limited, which can be a drawback in some applications.

Another important characteristic of a dynamical system is Lyapunov Exponent, which is a quantitative measure of chaos. A system is chaotic if the value of the Lyapunov exponent is strictly positive, as then a minor disturbance in the initial conditions may cause exponential divergence. The larger the Lyapunov exponent, the better is chaotic performance. Fig. 2(a) shows the variations of the Lyapunov exponent of the logistic map.



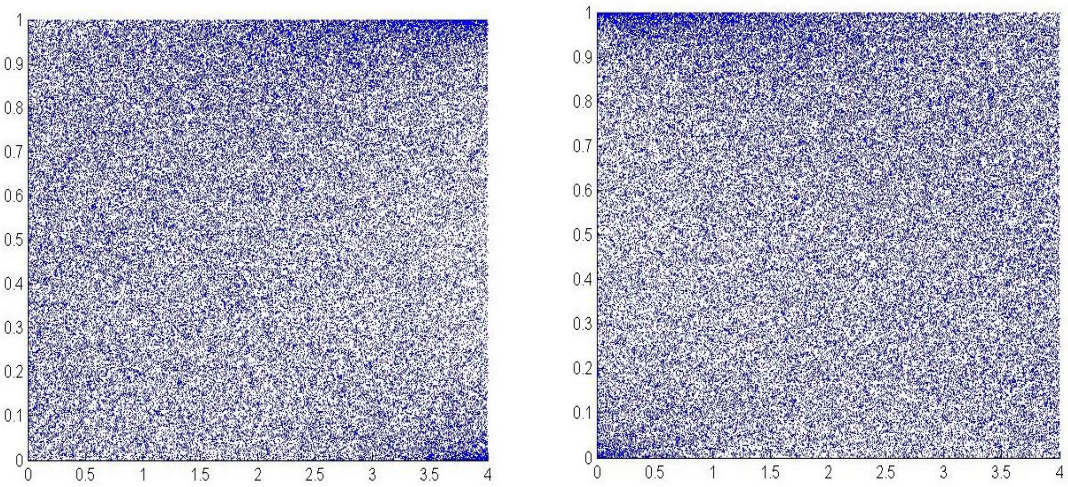
(a) (b)

Fig. 1. (a) Bifurcation diagrams of logistic map, (b) Bifurcation diagrams of sine map.



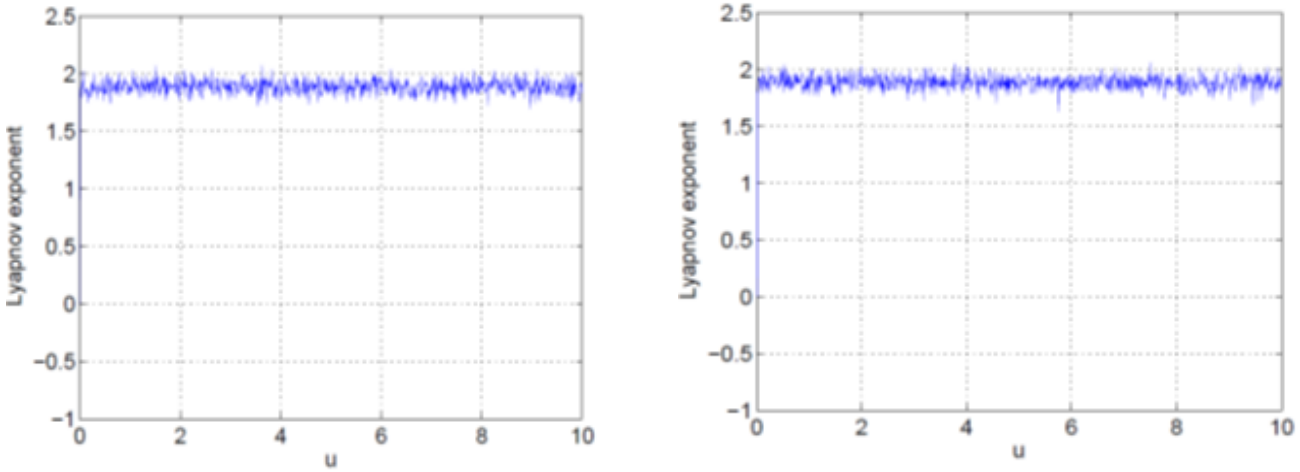
(a) (b)

Fig. 2. (a) Lyapunov exponents of logistic maps, (b) Lyapunov exponents of sine maps.



(a) LLS (b) SSS

Fig. 3. Bifurcation diagrams of LLS and SSS.



(a) LLS (b) SSS

Fig. 4. The Lyapunov exponent of LLS and SSS.

B. The Sine Map

It is a type of chaotic system that has received considerable attention in the area of nonlinear dynamics. It is a straightforward mathematical model that is capable of displaying intricate and unpredictable patterns. Sine map equation is represented as:

$$\mathcal{C}_{\mathcal{S}}(\vartheta_{\mathcal{S}}, x_i) = \frac{\vartheta_{\mathcal{S}} Sin(\pi x_i)}{4}; \quad (2)$$

Where $\vartheta_{\mathcal{S}} \in (0,4)$. Like the logistic map, the sine map also exhibits chaotic behavior. However, it has been observed that the chaotic range of the sine map is also limited, as shown in the bifurcation diagram presented in Fig. 1(b). The variations of the Lyapunov exponent of the sine map are shown in Fig. 2(b) Study regarding the combinations of one-dimensional chaotic maps shows that by introducing suitable combinations of such maps, the chaotic range can be enhanced [19]. In the next section, we discuss such combinations in detail.

C. Combinations of Chaotic Maps

Our approach involves creating new chaotic systems that have chaotic properties across their entire domain. We accomplish this by constructing nonlinear combinations of the underlying seed maps, which includes the LLS and SSS. The mathematical expression used for the nonlinear combination LLS is given below:

$$x_{i+1} = \mathcal{C}_{\mathcal{L}}(\vartheta_{\mathcal{L}}, x_i) \times \psi(n) - \mathcal{C}_{\mathcal{L}}(\vartheta_{\mathcal{L}}, x_i) \times \psi(n) - \lfloor \mathcal{C}_{\mathcal{L}}(\vartheta_{\mathcal{L}}, x_i) \times \psi(n) \rfloor; \quad (3)$$

Where $\psi(n) = 2^n$; $8 \leq n \leq 14$, is called an adjustment function. The larger the value of n, the better is the chaotic performance. For both LLS and SSS we choose n = 14. Eq. (3) can be rewritten as:

$$x_{i+1} = \vartheta_{\mathcal{L}} x_i (1 - x_i) \times 2^{14} - \lfloor \vartheta_{\mathcal{L}} x_i (1 - x_i) \times 2^{14} \rfloor \quad (4)$$

The figures depicting the bifurcation diagram and the Lyapunov exponent of the LLS chaotic system can be observed in Fig. 3(a) and Fig. 4(a), respectively. A comparison of the bifurcation diagram of LLS with that of the

logistic map in Fig. 2(a) reveals that the former exhibits a significantly wider chaotic range than the latter. Additionally, the improved uniform distribution of the density function in LLS compared to its seed maps ensures better chaotic behavior of the newly generated system and its efficient application in information security. The other two chaotic systems discussed in the following subsections exhibit similar properties. The expression for the Sine-Sine system can be obtained by using Eq. (1).

$$\mathcal{C}_S(\vartheta_S, x_i) == \frac{\vartheta_S Sin(\pi x_i)}{4} \times 2^{14} - \left\lfloor \frac{\vartheta_S Sin(\pi x_i)}{4} \times 2^{14} \right\rfloor \quad (5)$$

The bifurcation diagram and the variations of Lyapunov exponent are exhibited in Fig. 3(b) and Fig. 4(b). Just like the previous case, one may observe the improved performance of the new chaotic system.

III. Construction of Cryptographic S-Box

Block ciphers are cryptographic algorithms that convert plaintext into ciphertext by breaking it up into fixed-length blocks and applying a series of substitution and permutation operations. They are widely used to secure data in various applications, such as electronic payments, online transactions, and communication systems. S-boxes, or substitution boxes, are a key component of block ciphers, as they determine the nonlinear substitution of input bits with output bits in the encryption process. The quality of the S-box plays a vital role in the overall security of the cryptosystem, as any weakness or vulnerability in the S-box can be exploited by attackers to break the encryption. To achieve resistance against differential and linear cryptanalysis in an encryption scheme, the selection of a suitable S-box is crucial. Differential and linear cryptanalysis are two common techniques used by attackers to break ciphers, and a well-designed S-box can help to mitigate these attacks and provide stronger security. To ensure the highest level of security, cryptographers must carefully design and test S-boxes to ensure they are resistant to attacks and produce high-quality encryption output. The selection and design of S-boxes is a complex and ongoing research area, as the security requirements and threats to cryptosystems are constantly evolving. Despite the challenges, the use of strong and secure S-boxes is crucial for the development of robust and reliable cryptosystems.

Where $GL(n; \mathbb{F})$ are a group of invertible matrices and PGL of degree n over a field $\mathbb{F}$ is as $GL(n; \mathbb{F})$ by its center. We also form the 8×8 S-box through $GF(2^8)$ on $PGL(2, GF(2^8))$:

$$f : PGL(2, GF(2^8)) \times GF(2^8) \rightarrow GF(2^8)$$

Defined as:

$$\tau(z) = \frac{\alpha z + \beta}{\gamma z + \delta} \quad (6)$$

Here τ is LFT of $\in GF(2^8)$, which satisfying the non-degeneracy condition $\alpha\delta - \beta\gamma \neq 0$. Where $\alpha = 21$, $\beta = 8$ and $\gamma = 3$ and $\delta = 17$.

TABLE I. Constructed S-box

103	157	39	10	87	238	191	15	141	229	166	70	243	119	61	24
72	50	216	183	36	85	144	249	42	225	68	196	55	178	104	129
156	174	47	204	111	80	124	29	132	254	65	236	53	223	27	84
162	91	62	146	33	79	247	54	107	120	40	221	232	78	22	250
31	203	19	69	211	133	23	86	231	240	76	95	165	197	159	41
18	137	251	21	44	235	75	209	28	206	239	142	92	57	16	46
182	11	152	118	56	234	60	89	71	194	99	191	73	90	149	67
153	98	246	222	58	97	170	145	227	83	161	204	93	129	35	14
186	25	212	77	148	32	112	127	66	102	49	125	38	215	223	64
81	107	226	115	233	117	52	219	96	17	228	214	48	150	200	45
175	30	181	130	88	110	186	173	51	164	63	192	235	108	100	168
209	206	43	121	220	117	222	37	245	124	20	208	82	163	151	250
26	148	13	119	59	94	201	158	12	160	74	155	179	97	189	238
50	191	58	34	65	144	77	53	213	95	137	105	21	67	166	111
110	171	81	253	42	196	61	246	70	236	71	237	214	24	199	132
66	57	234	91	48	28	131	99	192	22	222	254	63	114	16	172

IV. Steganographic Scheme

The proposed scheme highlights some most essential steps for information embedding process. First, substituting the information through a highly nonlinear S-box. Secondly, instead of depending on either spatial or transform domain only, it employs a combination of both the domains to reach the acceptable level of embedding capacity as well as robustness. Thirdly, the scheme is based on stronger chaotic combinations which depict extraordinary features when compared with the individual seed maps. Lastly, it involves both DCT and DWT. The combined effect of both these transforms contributes to the robustness of the proposed method.

1) The detailed steganographic strategy is explained through the flowchart (Fig. 5). We explain the whole process in the following steps.

2) Take the host image (sized 512×512) in the spatial domain and shape it into a vector of length m.

3) Take the secret image $\mathcal{I}$ (to be embedded), that is $1/5$ of the host image size and substitute it using the S-box shown in table 1.

4) Break the substituted image into two parts $\mathcal{I}_{\infty}$ and $\mathcal{I}_{\in}$ in the ratio 70% and 30% respectively.

5) First, $\mathcal{I}_{\infty}$ is embedded at random positions of the host image, using the chaotic system *LLS*. This gives the partial stego image in the spatial domain.

6) Reshape this partial stego image into a matrix form and convert into the frequency domain by applying the combination of DWT and DCT.

7) Revamp the obtained image into a vector of length m and pick the largest frequency components (30% of the whole).

8) Use the chaotic system *SSS* to embed $\mathcal{I}_{\in}$ at the random positions of the selected largest values. This produces the frequency domain version of the stego image.

9) At this stage, apply the inverse of *DCT* and *DWT* to reach the final version of the stego image.

*10)*The original embedded image can be extracted from the stego image by applying the reverse of the above-explained method.

The simulation results are expressed in Fig. 6, Fig. 7. We apply the steganographic algorithm on two 512×512 images of baboon and Lena.

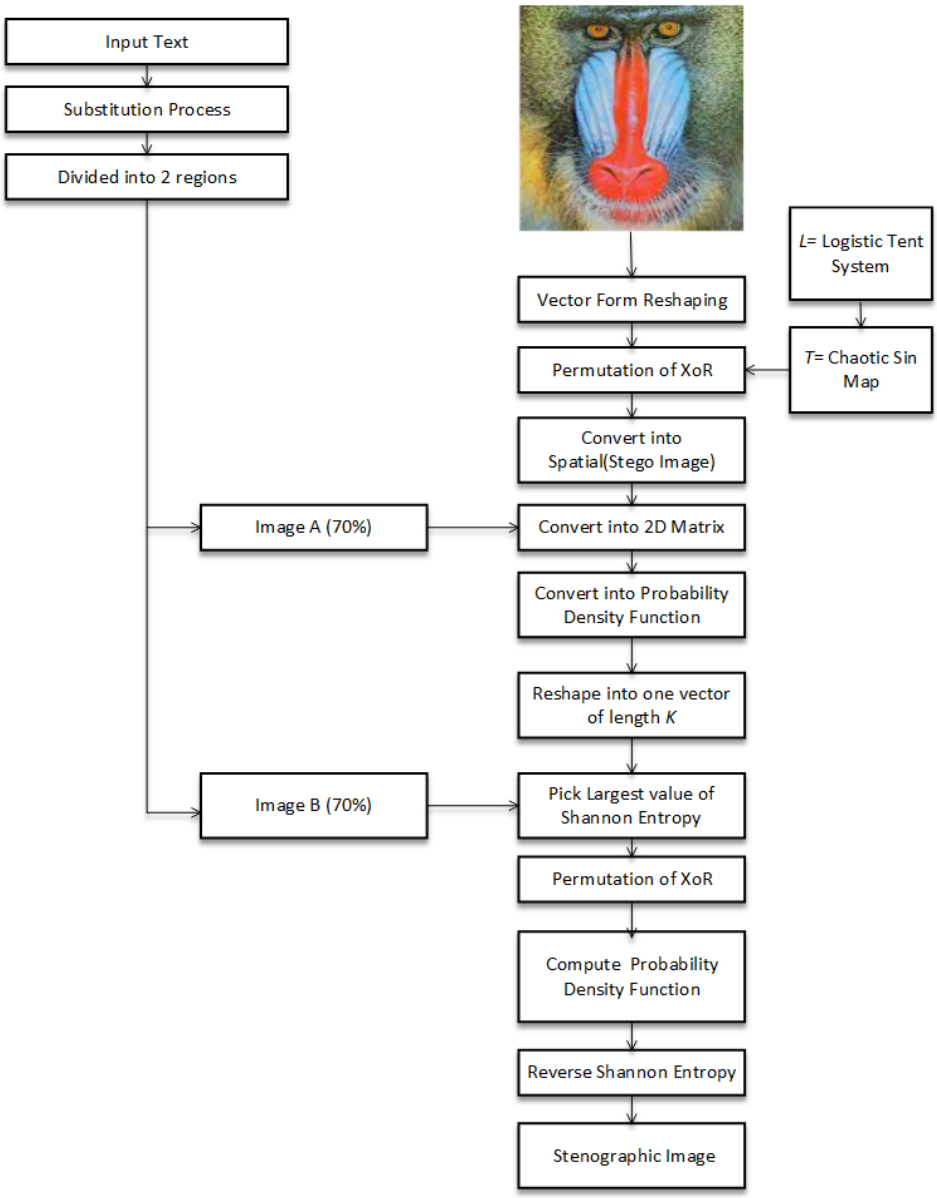
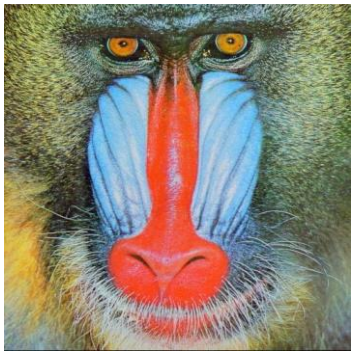
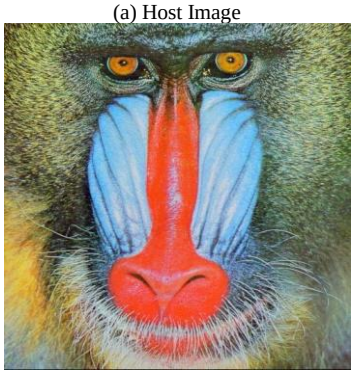


Fig. 5. Steganographic scheme.

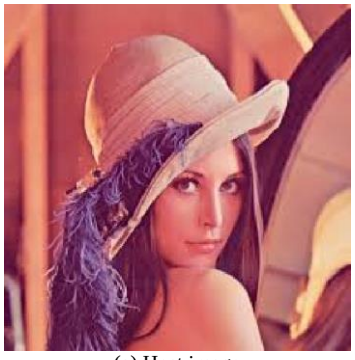


(a) Host Image



(b) Stego Image

Fig. 6. Stego images.



(a) Host image

(b) Stego image

Fig. 7. Host and stego images.

V. Statistical Security Analysis

In this section, we measure the cryptographic strength of the proposed scheme with the help of some useful analysis such as entropy, contrast, correlation, homogeneity, peak signal to noise ratio (PSNR) and mean squared error (MSE). We analyzed two benchmark images, baboon and Lena, using the proposed scheme. Notably, the scheme exhibits a remarkable feature of producing steganographic images that have high resemblance to their original counterparts. Moving on, let's discuss these security parameters one by one.

A. Contrast

The analysis of contrast is a method employed to evaluate the degree of sensitivity of image textures to variations in intensity. In simpler terms, it measures how much the texture of the image changes when the intensity of the image is changed. The contrast of an image is directly related to the texture of the image, and is an important factor in determining the quality of an image. Images with high contrast are usually considered to be of higher quality, since they have a greater range of intensity and a more distinct texture. The mathematical expression for the contrast is given as:

$$\text{Contrast} = \sum_i \sum_j |-j|^2 p(i,j), \qquad (7)$$

Where Table II and III present the values of contrast for each image, which are computed from the (i,j) th-element of GLCM represented by P(i,j).

B. Information Entropy

Entropy analysis is used to measure the randomness or the degree of disorder of a system. Entropy is a critical security parameter used to evaluate the strength of a cryptographic scheme. It is a measure of randomness or uncertainty in the data, indicating the degree of unpredictability in the scheme. In the context of steganography, entropy measures the level of randomness in the distribution of pixels in the steganographic image. A higher entropy value implies that the distribution of pixel values in the steganographic image is more random and unpredictable, making it harder for an attacker to identify the hidden data. In general, higher entropy values are desirable as they indicate a higher level of security. A scheme with a low entropy value is more predictable, and hence less secure, as it makes it easier for an attacker to detect the presence of hidden data. Therefore, a higher entropy value indicates a higher degree of randomness in the scheme and, consequently, a more secure scheme. However, achieving a high entropy value may not always be practical, as it can negatively impact the quality of the steganographic image. A scheme that produces high entropy values but produces a visually distinguishable steganographic image may not be useful in practice. Thus, a balance between high entropy values and image quality needs to be struck to ensure that the scheme is both secure and practical. The mathematical formula for information entropy is given by:

$$\text{Entropy} = -\sum_i \sum_j p(i,j) \log P(i,j), \qquad (8)$$

Tables II and III present the numerical outcomes for both the original and steganographic images. The algorithm we employed demonstrated favorable outcomes for entropy.

TABLE II. Original Image: Results of Majority Logic Criterion

Images	Entropy	Contrast	Correl.	Homog.
Baboon	5.4598	0.3389	0.9689	0.8753
Lena	5.3721	0.1342	0.9752	0.8654

TABLE III. STEGO IMAGE: RESULTS OF MAJORITY LOGIC CRITERION

Images	Entropy	Contrast	Correl.	Homog.
Baboon	5.6790	0.3409	0.9573	0.8845
Lena	4.9612	0.1217	0.9703	0.9603

C. Correlation

Correlation is another important security parameter used to evaluate the strength of a steganographic scheme. It measures the relationship between adjacent pixels in an image, indicating how much the pixel values are dependent on one another. A high correlation value implies that the adjacent pixel values are similar, and hence predictable, whereas a low correlation value indicates that adjacent pixels are less dependent on one another and more unpredictable. In steganography, a lower correlation value is desirable as it indicates a less predictable steganographic image, making it harder for an attacker to detect the hidden data. This is because the insertion of hidden data modifies the pixel values, disrupting the natural correlation between adjacent pixels. Therefore, a low correlation value indicates that the scheme is successful in hiding the data in the image, and thus more secure. However, it is important to note that achieving a low correlation value may not always be feasible, as it may come at the cost of image quality. If the scheme introduces too much noise or distortion into the image to reduce the correlation value, the resulting steganographic image may be of poor quality, making it distinguishable from the original image. Hence, a trade-off between low correlation and image quality needs to be achieved to ensure that the scheme is both secure and practical. Mathematical expression for correlation is given by:

$$Correlation = \sum_i \sum_j \frac{(i-E_X)(j-E_Y)}{D_X D_Y} p(i,j), \quad (9)$$

Where E_X, E_Y, D_X, D_Y represent the expected values and standard deviations of X and Y.

D. Homogeneity

Homogeneity is another security parameter that measures the uniformity of the intensity distribution in an image. It is a measure of the smoothness of the image, indicating how closely the pixel values are clustered around the average value. A higher homogeneity value indicates a more uniform distribution of pixel intensities in the steganographic image, making it more difficult for an attacker to detect the presence of hidden data. In the context of steganography, a high homogeneity value implies that the steganographic image closely resembles the original image, with minimal variation in pixel intensities. This is desirable as it indicates that the hidden data has been successfully embedded into the image without significantly altering its appearance. Thus, a high homogeneity value suggests a more secure scheme. However, as with other security parameters, achieving high homogeneity values while maintaining acceptable image quality can be challenging. A scheme that produces high homogeneity values but results in poor quality steganographic images may not be practical. Hence, a balance between high homogeneity and image quality needs to be achieved to ensure that the scheme is both secure and practical. The numerical results of the homogeneity analysis of the steganographic images are presented in Table II, providing a quantitative measure of the scheme's homogeneity. Its mathematical formula is:

$$Homogeneity = \sum_i \sum_j \frac{P(i,j)}{1+|i-j|} \quad (10)$$

E. Mean Squared Error

It is a security parameter used to evaluate the quality of a steganographic image. It measures the average squared difference between the pixel values of the original and steganographic images. A lower MSE value indicates a smaller difference between the original and steganographic images, and hence a higher quality steganographic image. In the context of steganography, a lower MSE value implies that the scheme has successfully embedded the hidden data into the image without significantly altering its appearance. This is because the scheme has introduced minimal distortion or noise into the image, resulting in a steganographic image that is visually similar to the original image. Thus, a low MSE value suggests a more secure scheme. However, achieving a low MSE value while maintaining high security can be challenging. A scheme that produces low MSE values but results in a visually distinguishable steganographic image may not be practical. Hence, a balance between low MSE values and image quality needs to be achieved to ensure that the scheme is both secure and practical. The numerical results of the MSE analysis of the steganographic images are presented in Table IV, providing a quantitative measure of the scheme's quality.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} X(i,j) - Y(i,j))^2, \quad (11)$$

Where $X(i,j)$ and $Y(i,j)$ represent the reference image and the steganographic image and i,j represents the pixel's position in an $M \times N$ image.

TABLE IV. MSE AND PSNR

Image	MSE	PSNR
Baboon	0.0024	58.2405
Lena	0.0017	57.6436

F. Peak Signal to Noise Ratio

It is a security parameter that measures the quality of a steganographic image by comparing the maximum possible signal value with the level of noise or distortion introduced by the embedding of hidden data. A higher PSNR value indicates a higher quality steganographic image with less noise or distortion. In steganography, a higher PSNR value indicates that the scheme has successfully hidden the data in the image without significantly degrading its quality. This is because a high PSNR value implies that the steganographic image is visually similar to the original image, with minimal distortion or noise. Thus, a high PSNR value suggests a more secure scheme. However, achieving high PSNR values while maintaining acceptable security can be challenging. A scheme that produces high PSNR values but results in a visually distinguishable steganographic image may not be practical. Hence, a balance between high PSNR values and security needs to be achieved to ensure that the scheme is both secure and practical. The numerical results of the PSNR analysis of

the steganographic images are presented in Table II, providing a quantitative measure of the scheme's quality. Where, a maximum pixel value in the image is given by MAX_I . PSNR is defined by:

$$\text{PSNR} = 20 \log_{10} \frac{\text{MAX}_\text{I}}{\sqrt{\text{MSE}}} \quad (12)$$

G. Robustness Analysis

To assess the resilience of the suggested steganographic technique, we perform several tests such as applying JPEG compression, adding noise, and cropping effect on the steganographic images. We determine the resemblance between the extracted steganographic image and the original one. Our algorithm's robustness is demonstrated by the high correlation between these two images. Mathematically, the estimation of similarity can be expressed as:

$$\text{Similarity measure} = \frac{\sum \text{r}_\text{i}\text{s}_\text{i}}{\sqrt{\text{r}_\text{i}^{\,2}\text{s}_\text{i}^{\,2}}} \quad (13)$$

Where r_i and s_i represent the corresponding elements. In the subsequent subsections, we will examine the impact of individual image processing operations one by one.

TABLE V. SIMILARITY UNDER VARIOUS ATTACKS

Attacks	Baboon	Lena
Compression	1.1124×10^{-4}	1.1125×10^{-4}
Noise	1.0906×10^{-4}	1.0957×10^{-4}
Cropping	1.1087×10^{-4}	1.1087×10^{-4}

H. JPEG Compression

In steganography, it is important to evaluate the robustness of the proposed scheme under different scenarios, including image compression. JPEG compression is a widely used lossy compression algorithm that can introduce significant distortion in the image, which may result in loss of hidden data. Therefore, it is crucial to test the proposed scheme's robustness under JPEG compression.

To evaluate the effect of JPEG compression on the steganographic images, we subjected the steganographic images of baboon and Lena to JPEG compression and studied the resultant images. The results of the study are presented in Fig. 8(a) and Fig. 9(a), which show the steganographic images before and after JPEG compression. Additionally, Table V presents the numerical results of the study, which prove the robustness of our proposed scheme. The results of the study demonstrate that the proposed scheme is robust to JPEG compression, as the hidden data remains intact even after compression. This is evidenced by the high values of security parameters such as entropy, correlation, homogeneity, PSNR, and low values of MSE for the compressed steganographic images. Thus, the proposed scheme is suitable for secure data transmission over channels that may introduce compression, such as the internet, where image compression is commonly used to reduce transmission time and bandwidth requirements.

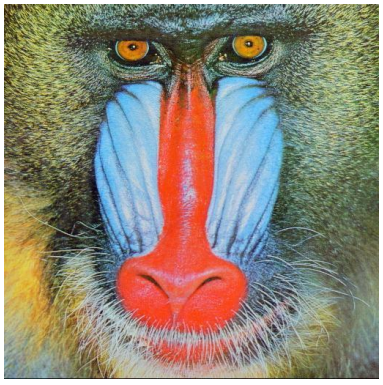
I. Noise Addition

In addition to evaluating the robustness of the proposed scheme under JPEG compression, it is important to assess its performance under other forms of image degradation, such as noise. Salt and pepper noise is a common form of noise that can affect the steganographic images during transmission, and it is important to ensure that the proposed scheme is robust against such attacks.

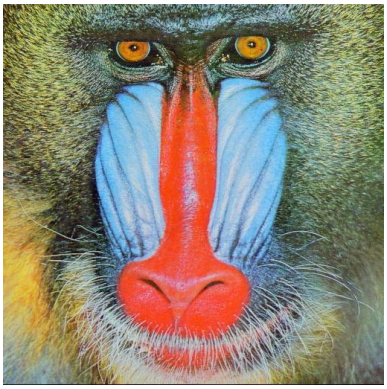
To evaluate the effect of salt and pepper noise on the steganographic images, we subjected the steganographic images of baboon and Lena to varying levels of noise and studied the resultant images. The results of the study are presented in Fig. 8(b) and Fig. 9(b), which show the steganographic images before and after applying salt and pepper noise. Additionally, Table V presents the numerical results of the study, which demonstrate the proposed scheme's robustness against noise attacks. The results of the study indicate that the proposed scheme is quite robust against salt and pepper noise attacks, as the hidden data remains intact even after the introduction of noise. The high values of security parameters such as entropy, correlation, homogeneity, and PSNR, and the low values of MSE for the steganographic images with noise, suggest that the scheme can effectively protect the hidden data from being compromised.

J. Cropping Effect

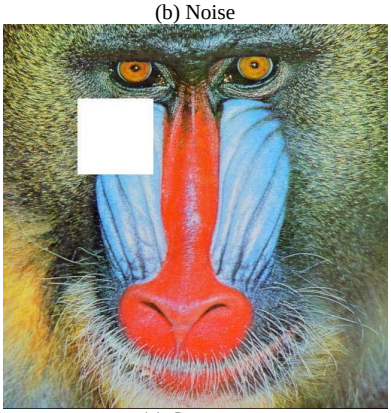
The cropping effect is an important consideration in evaluating the effectiveness of a steganographic scheme. The cropping of an image refers to the removal of a portion of the image, which can be used to hide the secret data. Therefore, it is essential to assess the robustness of the steganographic scheme against cropping attacks. To evaluate the cropping effect on the proposed scheme, we cropped the steganographic images of baboon and Lena left side. Cropped image is shown in Fig. 8(c) and Fig. 9(c) respectively. Table V presents the numerical results of the study, which demonstrate the robustness of the proposed scheme against cropping attacks. The results of the study indicate that the proposed scheme is quite robust against cropping attacks, as the hidden data remains intact even after the removal of a significant portion of the image. The high values of security parameters such as entropy, correlation, homogeneity, and PSNR, and the low values of MSE for the steganographic images with different cropping percentages, suggest that the scheme can effectively protect the hidden data from being compromised.



(a) Compression



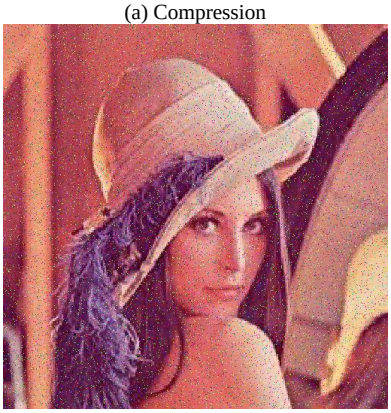
(b) Noise



(c) Cropping

Fig. 8. Baboon's image subjected to different image processing techniques.

(a) Compression



(b) Noise

(c) Cropping

Fig. 9. Lena's image subjected to different image processing techniques.

VI. Conclusion

Based on the proposed steganographic algorithm using enhanced chaotic maps, the results of the statistical security analysis demonstrate its robustness and high capacity for securely embedding secret information with good visual quality. The use of a novel fusion technique based on logistic and sine maps in constructing the cryptographic substitution box overcomes existing vulnerabilities of chaotic maps such as frail chaos, finite precision effects, dynamical degradation, and limited control parameters. The algorithm's statistical strength was assessed through several tests, including measures of information entropy, correlation, contrast, energy, homogeneity, peak signal-to-noise ratio, mean squared error, as well as evaluations of the algorithm's performance under JPEG compression and image degradation. These tests demonstrate the algorithm's ability to resist various attacks while maintaining good visual quality. In summary, the proposed steganographic algorithm satisfies the fundamental objectives of achieving both robustness and high-capacity for hidden information, and it offers a secure and effective means of embedding secret information in digital images. The algorithm's strengths in terms of security and visual quality make it a promising tool for applications where the protection of sensitive information is critical.

References

[1] Khan, Muhammad Fahad, et al. "A novel design of cryptographic SP-network based on gold sequences and chaotic logistic tent system." IEEE Access 7 (2019): 84980-84991.

[2] M. Fahad Khan, K. Saleem, M. Alotaibi, M. Mazyad Hazzazi, E. Rehman et al., "Construction and optimization of trng based substitution boxes for block encryption algorithms," Computers, Materials & Continua, vol. 73, no.2, pp. 2679–2696, 2022.

[3] Khan, Muhammad Fahad, Faisal Baig, and Saira Beg. "Steganography between silence intervals of audio in video content using chaotic maps." Circuits, Systems, and Signal Processing 33 (2014): 3901-3919.

[4] Khan, Muhammad Fahad, Adeel Ahmed, and Khalid Saleem. "A novel cryptographic substitution box design using Gaussian distribution." IEEE Access 7 (2019): 15999-16007.

[5] S. T., & Arivazhagan, S. (2019). Universal secret payload location identification in spatial LSB stego images. Annals of Telecommunications, 74(5-6), 273-286.

[6] Siddiqui, Ghazanfar Farooq, et al. "A dynamic three-bit image steganography algorithm for medical and e-healthcare systems." IEEE Access 8 (2020): 181893-181903.

[7] Martín, Alejandro, et al. "Evolving Generative Adversarial Networks to improve image steganography." Expert Systems with Applications (2023): 119841.

[8] Martín, Alejandro, et al. "Evolving Generative Adversarial Networks to improve image steganography." Expert Systems with Applications (2023): 119841.

[9] Daoui, Achraf, et al. "Color stereo image encryption and local zero-watermarking schemes using octonion Hahn moments and modified Henon map." Journal of King Saud University-Computer and Information Sciences 34.10 (2022): 8927-8954.

[10] Gakam Tegue, Gabriel Armand, et al. "A Novel Image Encryption Scheme Combining a Dynamic S-Box Generator and a New Chaotic Oscillator with Hidden Behavior." Arabian Journal for Science and Engineering (2023): 1-20.

[11] Alkhayyat, Ahmed, et al. "A novel 4D hyperchaotic system assisted josephus permutation for secure substitution-box generation." Journal of Signal Processing Systems 94.3 (2022): 315-328.

[12] Tanveer, Muhammad, et al. "Towards a secure and computational framework for internet of drones enabled aerial computing." IEEE Transactions on Network Science and Engineering (2022).

[13] Baig, Faisal, et al. "Onion steganography: a novel layering approach." Nonlinear Dynamics 84 (2016): 1431-1446.

[14] Shah, Tariq, Ayesha Qureshi, and Muhammad Fahad Khan. "DESIGNING MORE EFFICIENT NOVEL S 8 S-BOXES." International Journal on Information Technologies & Security 12.2 (2020).

[15] Kaur, Ishleen, et al. "An integrated approach for cancer survival prediction using data mining techniques." Computational Intelligence and Neuroscience 2021 (2021).

[16] Manzoor, Atif, Amjad Hussain Zahid, and Malik Tahir Hassan. "A new dynamic substitution box for data security using an innovative chaotic map." IEEE Access 10 (2022): 74164-74174.

[17] Khan, Muhammad Fahad, et al. "Human Psychological Disorder towards Cryptography: True Random Number Generator from EEG of Schizophrenics and Its Application in Block Encryption's Substitution Box." Computational Intelligence and Neuroscience 2022 (2022).

[18] Ahmad, Musheer, et al. "An image encryption algorithm based on new generalized fusion fractal structure." Information Sciences 592 (2022): 1-20.

[19] Khan, Muhammad Fahad, et al. "Block Cipher's Substitution Box Generation Based on Natural Randomness in Underwater Acoustics and Knight's Tour Chain." Computational Intelligence and Neuroscience 2022 (2022).

[20] Khan, Muhammad Fahad, et al. "Multilevel information fusion for cryptographic substitution box construction based on inevitable random noise in medical imaging." Scientific reports 11.1 (2021): 1-23.