JOURNAL OF THEORETICAL PHYSICS & CRYPTOGRAPHY

www.IJTPC.org/Publications

A GUI Model to Encrypt Messages Using Chaotic Cipher and its Cryptanalysis

Mina Mishra, V.H. Mankar

Ph. D. Scholar, Electronics & Telecommunication, Nagpur University, Nagpur, Maharashtra, India
Lecturer, Electronics Engineering, Government Polytechnic, Nagpur, Maharashtra, India

ABSTRACT

In this paper the development of GUI to encrypt messages with message-embedded Scheme based chaotic cipher and its cryptanalysis against various attacks is presented. The designed ciphers use different chaotic maps like Logistic, Duffings, Arnolds Cat, Henon and Burger and named according to the chaotic map used in it. The GUI allows encrypting the plaintext by any of the developed cipher and crypt analyzes the cipher for particular message for plaintext sensitivity, key sensitivity, identifiability and known plaintext attack. The generated cipher text can be sent through an insecure channel, so that would be very difficult to be interpreted by an intruder or attacker. At the end of the communication, the recipient can decrypt the original message using the secret key.

Keywords

Chaotic cryptography, Chaotic maps, Cryptanalysis, Software.

1. INTRODUCTION

Cryptography which is the science of scrambling messages has its roots since ancient times. The relationship between chaotic dynamical systems and cryptography makes it natural to employ it to design new cryptosystems. It is based on the fact that chaotic signals are noise like and very sensitive to initial conditions. The sensitivity to initial conditions and spreading out trajectories over the whole model seems to be the model that satisfies the classic Shannon requirements of confusion and diffusion. Chaotic maps and cryptographic algorithms (or more generally maps defined on finite fields) have also some similar properties: sensitivity to initial conditions and parameters, random like behavior and unstable orbits with long periods, depending upon the precision of the numerical implementation [1]. Encryption rounds of a cryptographic algorithm lead to the desired diffusion and confusion properties of the algorithm. In a similar manner, iterations of the chaotic map spread the initial region over the entire phase space while the parameters of the chaotic map may represent the key of the encryption algorithm. Applications of chaotic maps to cryptography have some good fundamental properties such as a random like nature, mixing properties and sensitivity to changes in initial conditions and parameters [2]. Chaos-based encryption is an efficient and hot research aspect considering virtues of chaotic sequence. It is well known that chaotic sequences are pseudorandom, non-periodic, unpredictability, and especially sensitive to initial parameters, or say good avalanche effect. These features are very important for modern cipher algorithms, especially for stream ciphers [3].

This paper aims towards developing GUI which can encrypt any message using the developed ciphers and then each of the ciphers is further crypt analyzed for linear, differential attacks and brute-force attacks for that particular message. Another GUI developed can also decrypt cipher texts from database to original information if it has been encrypted using the developed ciphers.

It is concluded that the GUI is very much worth in encryption of messages and testing the validation of the developed ciphers within minimum possible time in seconds or a minutes . In future more number of developed ciphers and cryptanalytic procedures can be incorporated.

The paper is organized in the way as follows: Section II briefs the method used in the development of ciphers. Section III & IV discusses about the chaotic maps and non-Linear functions used in designing of ciphers. The next section describes the cryptanalysis procedures developed to test the validation of

the ciphers. Section VI gives the GUI developed and further sections shows some of the obtained results and then conclusion and future scope has been discussed.

2. MESSAGE-EMBEDDED SCHEME BASED CHAOTIC CIPHER

The message embedding scheme in the discrete time case, involves the transmitter system Σ_θ given by the general form

$$\Sigma_\theta \begin{cases} x_{k+1} = f_\theta(x_k, m_k) \\ y_k = h_\theta(x_k, [m_k]) \end{cases} \quad \ldots(1)$$

Where $x_k \in X \subset R^n$ is the state vector, $y_k \in y \subset R$ the measured, and so available, output, $m_k \in M \subset R$ the information signal, f_θ is a nonlinear chaotic function and h_θ a (possibly) nonlinear function, both parameterized by θ, $\theta = [\theta^{(1)}, \ldots, \theta^{(L)}]^T \in \Theta \subset R^L$, the parameter vector? The most common nonlinearities f_θ are of polynomial type (Henon map, Logistic map, Arnold's cat map …). $[m_k]$ means that h_θ can depend on m_k but not necessary. The initial condition of x_k will be denoted x_0. At the receiver side, the information recovering requires a synchronization mechanism [4].

3. GENERATION OF CHAOTIC MAPS

The chaotic maps used in designing of ciphers are 1-D Logistic map, 2-D Burger map, Arnolds Cat map, Henon map and Duffings map. Different combinations of non-linear and chaotic maps have been used to design the ciphers [5].

A. Logistic: The logistic map is a polynomial mapping of degree 2, it takes a point, in a plane and maps it to a new point using following expressions:

$$x(k+1) = r$$
$$x(k)(1 - x(k)) \quad \ldots(2)$$

Where, map depends on the parameter r. From r = 3.57 to r = 4, the map exhibits chaotic behavior which is shown in fig 1.

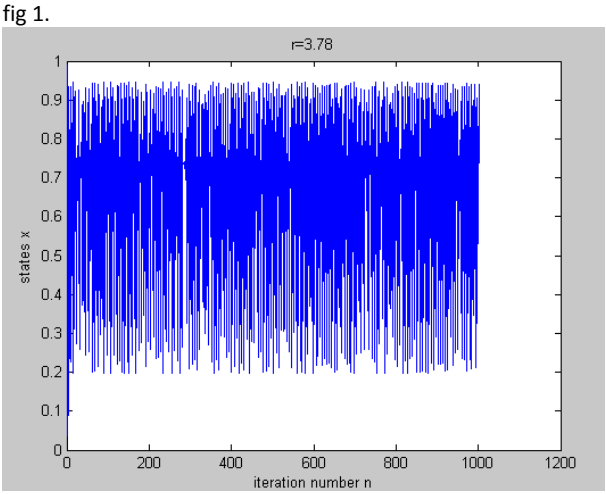

Fig. 1: Plot of Logistic map for r = 3.78, x(0) = 0.99, n = 1000.

B. Duffings: The Duffings map is a 2-D discrete-time dynamical system, which takes a point (x, y) in the plane and maps it to a new point using equations:

$$x(k+1) = y(k)$$
$$y(k+1) = -bx(k) + ay(k) - y^3(k) \quad \ldots(3)$$

a and b are parameters on which the map depends. The map exhibits chaotic nature as shown in fig 2.

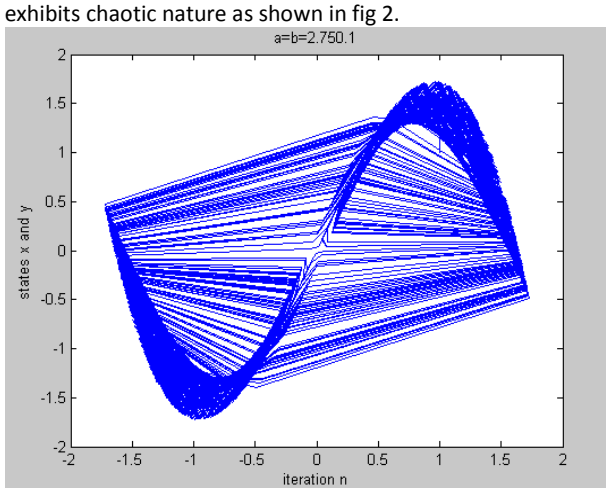

Fig. 2: Plot of Duffings Map at x(0) = - 0.04, y(0) = 0.2, a= 2.75, b=0.1, n=1000.

C. Arnolds Cat: The Arnolds Cat map is a 2-D discrete-time dynamical system, which takes a point(x, y) in the plane and maps it to a new point using equations:

$$x(k+1) = (a-1) \bmod (2x(k) + y(k), N)$$
$$y(k+1) = \bmod (x(k) + (1-b)\, y(k), N) \quad \ldots(4)$$

a and b are parameters on which the map depends. The map exhibits chaotic nature as shown in fig 3.

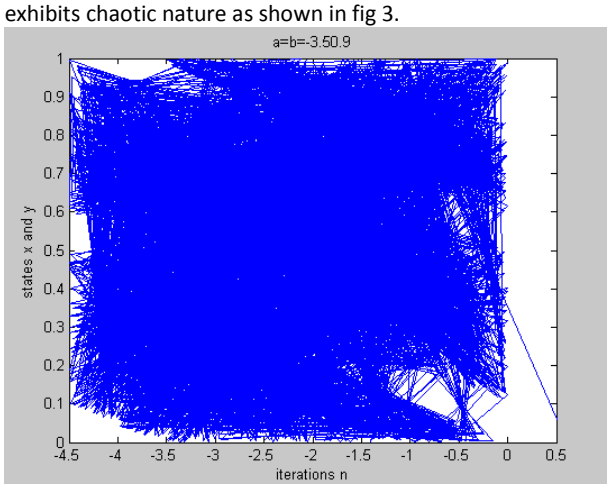

Fig. 3: Plot of Arnolds Cat Map at x(0) = 0.5, y(0) = 0.06, a = - 3.5, b = 0.9, n=5000.

D. Henon: The Henon map is a discrete-time dynamical system. The Henon map takes a point (x, y) in the plane and maps it to a new point using following equations:

$$x(k+1) = a\, x^2(k) + by(k)$$
$$y(k+1) = c\, x(k) + d \quad \ldots(5)$$

The map depends on four parameters a, b, c and d. Hénon map is chaotic as shown in fig 4.

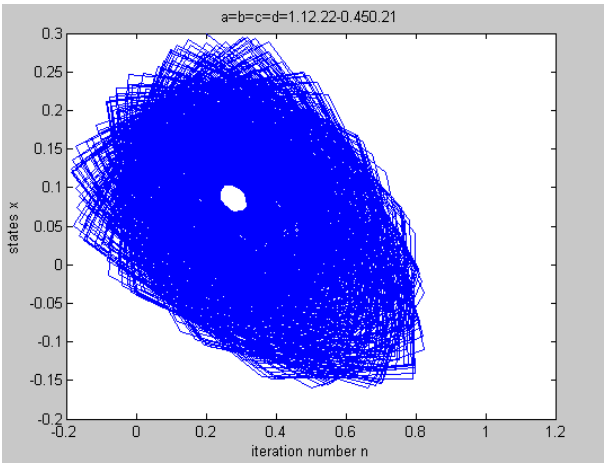

Fig. 4: Plot of Henon Map at x(0) = 0.2, y(0) = 0.3, a = 1.1, b = 2.22, c = - 0.45, d = 0.21, n=5000.

E. Burger: The Burger map is a 2-D discrete-time dynamical system, which takes a point(x, y) in the plane and maps it to a new point using equations:

$$x(k+1) = (1- b)\, x(k) - y^2(k)$$

$$y(k+1) = (1+ a)\, x(k) + x(k)y(k) \quad \ldots(6)$$

a and b are parameters on which the map depends. The map exhibits chaotic nature as shown in fig 5.

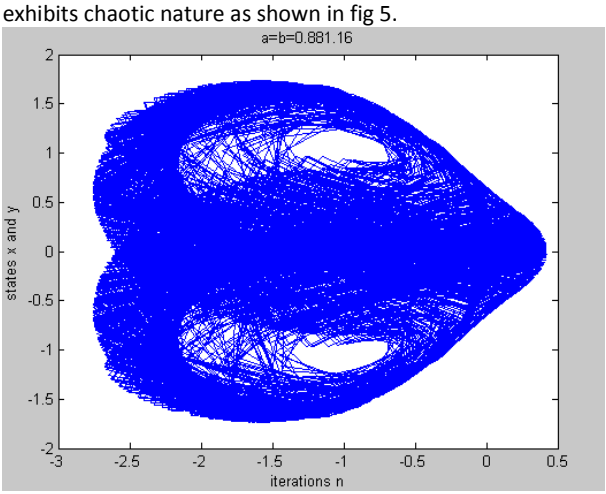

Fig. 5: Plot of Burger Map at x(0) = - 0.042365, y(0) = 0.27569, a = 0.88, b = 1.16, n=5000.

4. NON-LINEAR FUNCTIONS

Non-linear functions used in this work are discussed here in brief.

A. Sinusoidal: The sine function that describes a smooth repetitive oscillation. Its most basic form as a function of time (t) is:

$$Y(t) = A \sin(wt + \phi) \quad \ldots(7)$$

Where, A, the amplitude is the peak deviation of the function from its center position. ω, the angular frequency, specifies how many oscillations occur in a unit time interval, in radians per second . ϕ, the phase, specifies where in its cycle the oscillation begins at t = 0.

B. Exponential: The exponential function is the function ex, where e is the number (approximately 2.718281828) such that the function ex equals its own derivative. The exponential function is used to model phenomena when a constant change in the independent variable gives the same proportional change (increase or decrease) in the dependent variable.

C. Mod: The Mod numeric function returns returns the remainder when the dividend is divided by the divisor. The result is negative only if the dividend is negative. Both the numbers must be integers. The function returns an integer. If any number is NULL, the result is NULL. For example:

Mod (5, 3) returns 2.

Mod (-5, 3) returns -2.

D. Non-linear Feedback Register: A NLFSR (Non-Linear Feedback Shift-register) is a common component in modern stream ciphers, especially in RFID and smartcard applications. NLFSRs are known to be more resistant to cryptanalytic attacks than Linear Feedback Shift Registers (LFSR's), although construction of large NLFSRs with guaranteed long periods remains an open problem. A NLFSR is a shift register whose current state is a non-linear function of its previous state. The NLFSR used here is shown in fig 8.

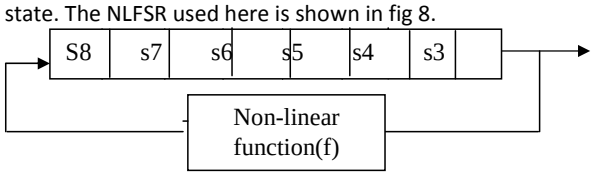

Fig. 6: NLFSR using 8-bit shift register

5. CRYPTANALYSIS

Cryptanalytic procedures refer to the methods applied on ciphers to analyze its security against the attacks [6]. Four methods of cryptanalysis developed are applied which are discussed in brief as follows:

A. Key Space Analysis: The size of the key space is the number of encryption/decryption key pairs that are available in the cipher system [7]. In the designed ciphers, the key space (range of keys) is defined clearly. Key space belongs to the chaotic region of the system. The total key space is a product of all the parameters involved. Once the key has been defined and key space has been properly characterized, the good key is chosen randomly from the large key ranges.

B. Identifiability Test:

Definition 1: An input sequence over a window of iterations $[0-T]$, denoted by $\{m_k\}_0^T$, is called an admissible input on $[0-T]$ if the difference equation (1) admits a unique local solution.

Definition 2: The system Σ_θ is locally strongly x_0- identifiable at θ through the admissible input sequence $\{m_k\}_0^T$ if there exists an open neighborhood of $\theta, v(\theta) \subset \Theta$, such that for any $\hat{\theta} \in v(\theta)$ and for any $\theta \in v(\theta)$

$$\hat{\theta} \neq \theta \Rightarrow \{y_k(x_0, m_k, \hat{\theta})\}_0^T \neq \{y_k(x_0, m_k, \theta)\}_0^T \quad \ldots(8)$$

Definition 3: The system Σ_θ is structurally identifiable if there exist $T > 0$, an open subset $X_0 \subset X$ and some dense subsets $sv(\theta) \subset \Theta$ and $M_0^T \subset M$, such that, for every $x_0 \in X_0, \theta \in v(\theta)$ and $\{m_k\}_0^T \in M_0^T$, the system Σ_θ is locally strongly x_0- identifiable at θ through the admissible input sequence $\{m_k\}_0^T$.

In the definitions above, the subset X_0 is open in order to avoid considering an a typical set of zero measure which

leads to singularities and where no conclusion about identifiability is possible. Moreover, these definitions are given for the initial condition taken at the particular time step k = 0. However, we can consider any time step k because the system (1) is shift-invariant.

The Definition 3 is a direct discrete-time counterpart of that of the structural identifiability of continuous-time systems, given in and is equivalent to the definition of rational identifiability.

To test the identifiability of system parameters, an approach, the outputs equality approach is performed.

Outputs Equality Approach: The outputs equality approach is directly based on Definition 3. The trajectories $y_k(\theta)$ contain information about the unknown parameter vector θ. The approach consists in testing whether the equality of the output trajectories of systems Σ_θ and $\Sigma_{\hat{\theta}}$, over an iteration window $[0-T]$, implies the equality of the parameter vectors θ and $\hat{\theta}$. So, the following theorem states a sufficient condition for structural identifiability of system (1).

Theorem 1: The system Σ_θ (1) is structurally identifiable if the set of equations

$$\{y_k(x_0, m_k, \hat{\theta})\}_0^T = \{y_k(x_0, m_k, \theta)\}_0^T \quad \text{...(9)}$$

has a unique solution for $\hat{\theta}$, that is $\hat{\theta} = \theta$.

T is a positive integer and represents the number of iterations required to prove that $\Rightarrow \hat{\theta} = \theta$. If T goes to infinity and the previous relation cannot be proved, no conclusion on structural identifiability can be given. As T is unknown a priori, Theorem 1 is only a sufficient condition of structural identifiability.

Besides, to recover θ, Theorem 1 requires the knowledge of the initial condition.

A. Plaintext Sensitivity: It is the percentage of change in bits of cipher text obtained after encryption of plaintext, which is derived by changing single bit from the original plaintext from the bits of cipher text obtained after encryption of original plaintext. With the change in single bit of plaintext, there, must be ideally 50% change in bits of cipher text to resist differential cryptanalysis (chosen-plaintext attack) and statistical analysis[8].

B. Key Sensitivity: Key sensitivity is the percentage of change in bits of cipher text obtained after encryption of plaintext using key, which is flipped by single bit from the original key, from bits of cipher text obtained after encryption of plaintext using original key, which requires ideally 50% change in cipher text bits to resist linear and statistical attacks [9].

C. Known plaintext attack: For observing this attack on developed ciphers it is assumed that the opponent knows everything about the algorithm, he/she has the corresponding cipher text of plaintext and some portion of plaintext. With this much information, the opponent tries to find out the secret key [10].

6. GUI DEVELOPMENT

This section consists of the GUI'S developed to perform encryption using the developed ciphers. GUI makes the work user-friendly. Two GUI's have been developed as shown in fig 7 and 9.

As seen in fig 9, the user types the message in the box labeled as plaintext and then presses the particular labeled cipher to encrypt it. All the pushbuttons are required to be pressed by the user to get the particular function labeled on it to be done and result will be displayed in the window.

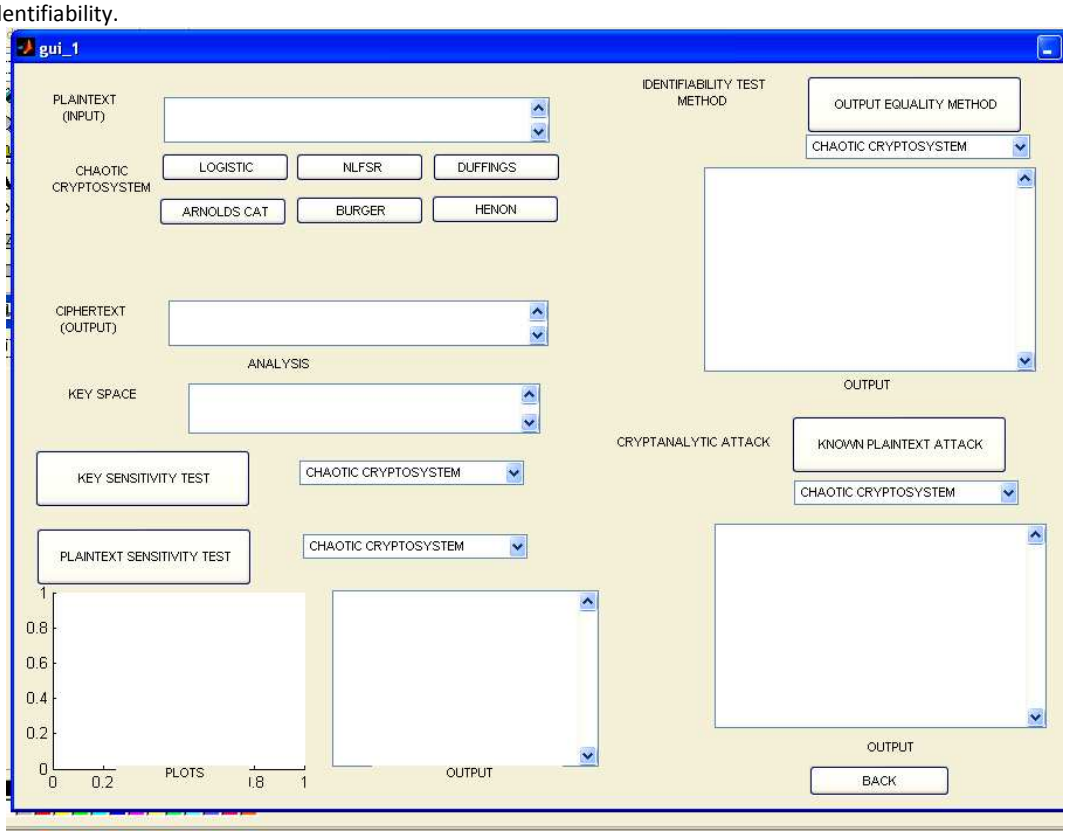

Fig. 7: Graphical user interface for analysis of chaotic text encryption method.

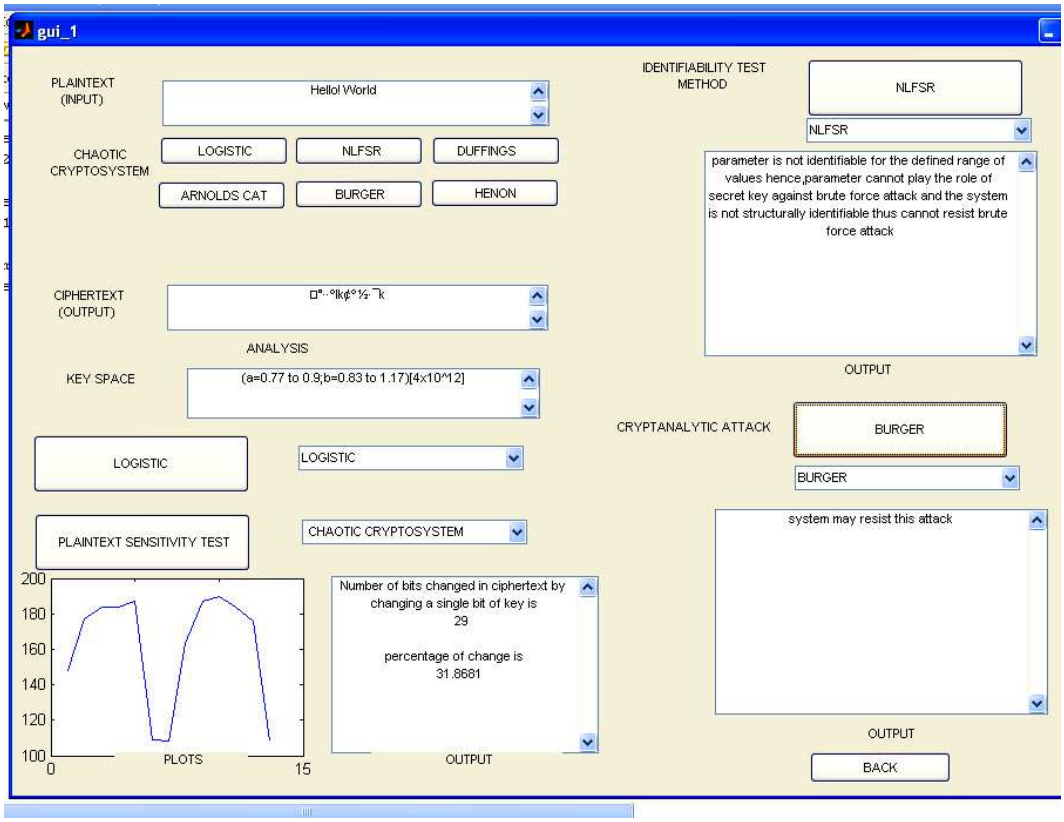

Fig. 8: Runned Graphical user interface for encryption and cryptanalysis

Fig. 8 shows the GUI with result displayed in the window for particular message "Hello World!"

Key space window displays the key space of cipher which has been used to encrypt the message.

Back pushbutton signifies to call next graphical user interface.

GUI shown in fig. 9 performs the detection of cipher text contained in the database and implements decryption part.

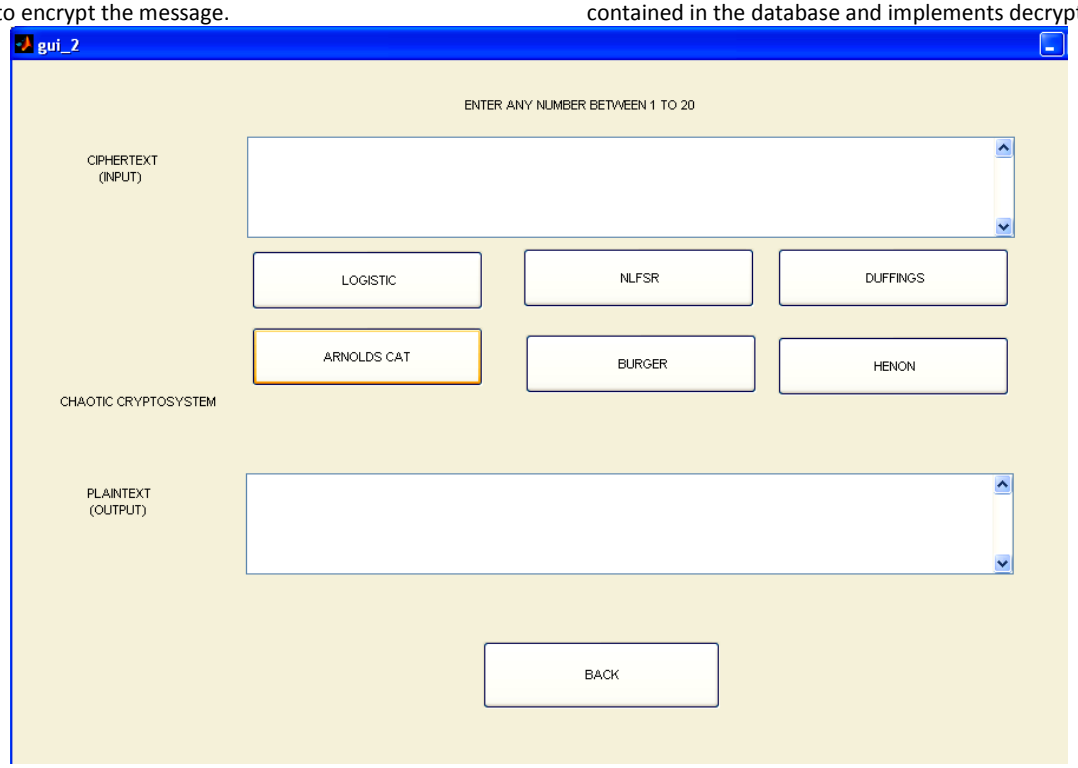

Fig. 9: Graphical user interface for detecting text encryption method from cipher text.

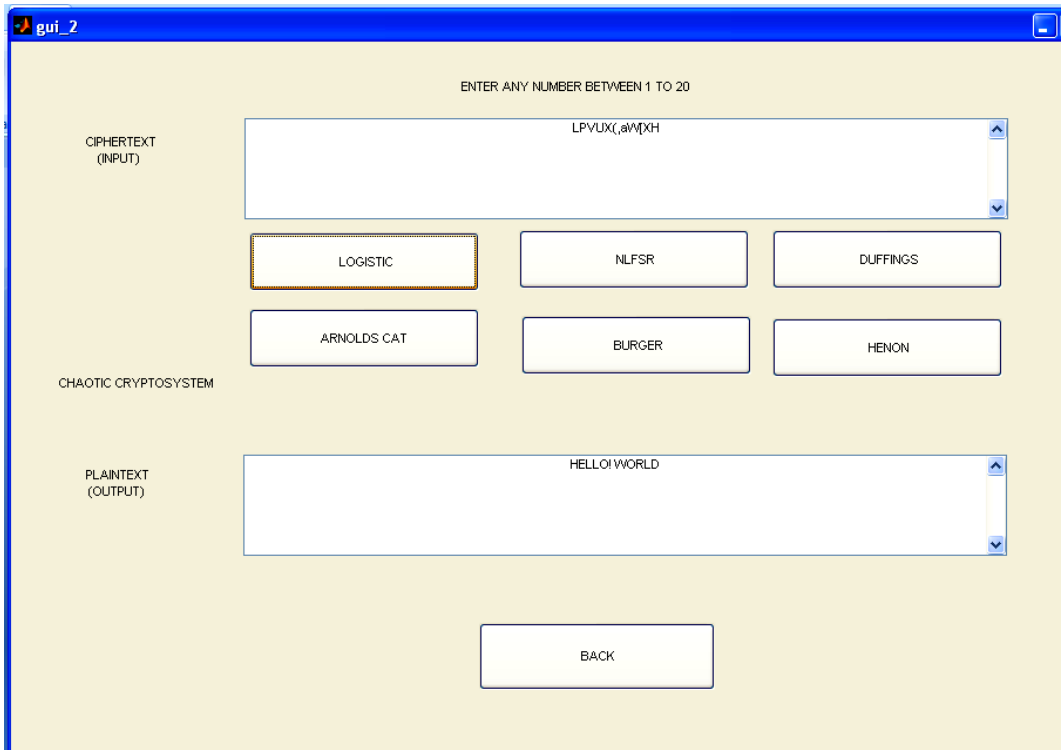

Fig. 10: Runned Graphical user interface for detection

GUI as shown in fig. 10 decrypts the cipher text which arrives in input from the database that contains at least 20 numbers of cipher texts. The cipher text obtained using any of the shown method is easily detected if decrypted plaintext has some meaningful statements or texts.

7. RESULTS

Some of the results obtained for various texts using each of the developed ciphers have been cited in the tables given in this section [11]-[15].

A. Logistic: Key Space range is from 3.57 to 4.0

Table 1: Analysis Table for Logistic cipher

Sl. No.	Plaintext	Key value	Cipher text	Plaintext sensitivity(in %)	Key sensitivity (in %)	Domain for key With increment =0.0001	Identifiability of key for iteration value =1 or 2	Robustness against known plaintext attack For p=[p1 p2]	Whether key can act as secret key against Brute Force attack?
1.	What is your name?	3.57	+bsl +t~+z}+ylxpJ	1.9737	13.8158	(3.57,3.77)	NI	R	NO
2.	I am going to market.	3.59	QGBFtt=qNt\>ShpK;v >>	3.6458	39.2045	(3.57,3.77)	NI	R	NO
3.	My college name is s.s.c.e.t.	3.6	;e4^Eyc@ky_t@aEjraK~a78vaz 49R_	2.9167	41.2500	(3.57,3.78)	NI	R	NO
4.	Hello!how are you?	3.65	BHZOR0Nhw`XVb?WoM	3.9474	46.7105	(3.57,3.78	NI	R	NO
5.	Sita is singing very well.	3.7	<nupBur{=c J}ZQ.3jTeZ[dA_	5.0926	37.9630	(3.67,3.87)	NI	R	NO

NI – Non-Identifiable; I – Identifiable; R – Robust; p [p1 p2… p n] – First 'n' characters of available plaintext string.

B. **Henon:** Key space is from [-0.9 2.19 -0.44 0] to[1.39 2.22 -0.45 0.277]

Table 2: Analysis table for Henon cipher

Sl. No.	Plaintext	Key value	Cipher text	Plaintext sensitivity (in %)	Key sensitivity (in %)	Domain for key With increment = 0.001	Identifiability of key for iteration value =2 or 3	Robustness against known plaintext attack For p= [p1 p2].	Whether key can act as secret key against Brute Force attack?
1.	How are you?	[-0.9 2.19 -0.44 0]	® ¶ _ ± ¤ _ ¸ ® ´ ~	0.8333	10.7692	[-0.9 2.19 -0.44 0] to [-0.895 2.195 -0.44 0.005]	I	R	YES
2.	Meet me after 5p.m.	[-0.85 2.19 -0.35 0.1]	_ 4o¤ X¤ X³ _ 4¬ 5¤ X_ 4 c¥ U³ ¤ X± _ 4t U¯ !m K¬ 5m K	0.8750	14.8750	[-0.85 2.19 -0.35 0.1] to [-0.795 2.195 -0.35 0.1]	I	R	YES
3.	I have a gift for you.	[-0.8 2.2 -0.35 0.15]	_ < _ <§ ± «µ ®¤ ¯ _ < «_ <¦ °¨ ±¥ ¯³ ° _ <¥ ¯® ³± ¯ ² <¸ ©® ³´ ¯m U	0.7609	15.2174	[-0.8 2.2 -0.35 0.15] to[-0.8 2.205 -0.245 0.15]	I	R	YES
4.	We will go for walk.	[-0.75 2.2 -0.35 0.15]	_ < ¤ ¸_ <¶ Ð© ¿« Ã« Ã_ <¦ ¼¯ Ç_ <¥ º¯ Ç± Ë_ <¶ Ð ²« Ã« Ân U	0.8333	13.5714	[-0.75 2.2 -0.35 0.15] to [-0.645 2.205 -0.35 0.15]	I	R	YES
5.	Study different papers.	[-0.6 2.18 -0.35 0.16]	U 2 t© $¤ª $¦ ® &¬U 2 - - § #¡ £ "© $¤U 2¥ " ¥ " § #¡¨ $£c C	0.8333	15.1042	[-0.6 2.175 -0.355 0.16] to[-0.6 2.18 - 0.35 0.16]	I	R	YES

6. **Burger:** Key space is from [0.77 0.83] to [0.9 1.17]

Table 3: Analysis Table for Burger cipher

Sl. No.	Plaintext	Key value	Cipher text	Plaintext sensitivity (in %)	Key sensitivity (in %)	Domain for key With increment = 0.0001	Identifiability of key for iteration value =2 or 3	Robustness against known plaintext attack for p=[p1 p2].	Whether key can act as secret key against Brute Force attack?
1.	How are you?	[0.71 0.84]	I»Ãl-¾±lÅ»Á	0.9615	24.0385	[0.71 0.84] to [0.715 0.841]	I	NR	YES
2.	Meet me after 5p.m.	[0.72 0.85]	k°°¿k¸°k¬±¿°½k»y¸y	1.8750	21.8750	[0.72 0.85] to [0.725 0.852]	NI	R	NO
3.	I have a	[0.73	kk³¬Á°k¬k²´±¿k±º½kÄºÀy	1.6304	26.0870	[0.73	I	NR	YES

Sl. No.	Plaintext	Key value	Cipher text	Plaintext sensitivity (in %)	Key sensitivity (in %)	Domain for key With increment = 0.0001	Identifiability of key for iteration value =2 or 3	Robustness against known plaintext attack for p=[p1 p2].	Whether key can act as secret key against Brute Force attack?
	gift for you.	0.86]				0.86] to [0.732 0.865]			
4.	We will go for walk.	[0.74 0.87]	m¤²mÄ¶¹¹m´¼m³¼¿mÄ®¹¸{	1.1905	23.8095	[0.74 0.87] to [0.742 0.875]	I	NR	YES
5.	Study different papers.	[0.75 0.88]	m ÁÂ±Æm±¶³³²¿²»Ám½®½² ¿À{	1.0417	28.1250	[0.75 0.88] to [0.755 0.882]	NI	R	NO

7. Duffings: Key space is from [1.8 -0.59] to [2.9 0.2]

Table 4: Analysis Table for Duffings cipher

Sl. No.	Plaintext	Key value	Ciphertext	Plaintext sensitivity (in %)	Key sensitivity (in %)	Domain for key With increment = 0.0001	Identifiability of key for iteration value =2 or 3	Robustness against known plaintext attack for p=[p1 p2].	Whether key can act as secret key against Brute Force attack?
1.	How are you?	[1.81 -0.44]	Ipx!bsf!zpv@	2.3810	0	[1.81 -0.44] to [1.81 -0.43]	NI	R	NO
2.	Meet me after 5p.m.	[1.82 -0.57]	!Nffu!nf!bgufs!6q/n/	1.4286	48.7500	[1.82 -0.57] to [1.83 -0.57]	NI	R	NO
3.	I have a gift for you.	[1.85 -0.47]	J!ibwf!b!hjgu!gps!zpv/	0.6494	50	[1.85 -0.47] to [1.85 -0.46]	NI	NR	NO
4.	We will go for walk.	[1.89 -0.3]	"Yg"yknn"iq"hqt"ycnm0	0.6803	0	[1.89 -0.3] to [1.9 -0.3]	NI	NR	NO
5.	Study different papers.	[1.9 0.2]	!Tuvez!ejggfsfou!qbqfst/	1.1905	0	[1.9 0.2] to [1.7 0.2]	NI	R	NO

8. Arnolds Cat: Key space is from [-5 0.4] to [-0.9 1.5]

Table 5: Analysis Table for Arnolds Cat cipher.

Sl. No.	Plain text	Key value	Ciphertext	Plaintext sensitivity (in %)	Key sensitivity (in %)	Domain for key With increment = 0.0001	Identifiability of key for iteration value =2 or 3	Robustness against known plaintext attack for p=[p1 p2].	Whether key can act as secret key against Brute Force attack?
1.	How are you?	[-5 0.4]	ºÂk¬½°kÄºÀ	3.1250	31.25	[-5.0 0.4] to [-4.995 0.4031]	NI	R	NO
2.	Meet me after 5p.m.	[-4 0.5]	¯¯¾j·¯j«°¾¯¼j ºx·x	2.6316	38.1579	[-4.0 0.5] to [-3.995 0.5031]	NI	NR	NO
3.	I have a gift for you.	[-3 0.6]	h°©¾-h©h¯±®¼h®·ºhÁ·½v	1.1364	24.4318	[-3. 00 0.6] to [-2.995 0.6031]	I	NR	YES
4.	We will go for walk.	[-2 0.7]	l£±lÃµ¸¸l³»l²»¾lÃ-¸·z	0.5952	31.5476	[-2 0.7] to [-1.995 0.0.7031]	NI	NR	NO
5.	Study different papers.	[-1 0.8]	¿À¯Äk¯´±±°½°¹¿k»¬»°½¾y	0.5435	31.2500	[- 1 0.8] to [-0.995 0.8031]	I	R	YES

9. CONCLUSIONS & FUTURE SCOPE

In this paper, we have presented the GUI to encrypt messages with message-embedded Scheme based chaotic cipher and its cryptanalysis against various attacks. The designed ciphers uses chaotic maps like Logistic, Duffings, Arnolds Cat, Henon and Burger and named according to the chaotic map or non-linear function used in it. The GUI allows encrypting the plaintext by any of the developed cipher and crypt analyzes the cipher for particular message for plaintext sensitivity, key sensitivity, identifiability and known plaintext attack. The generated cipher text can be sent through an insecure channel, so that would be very difficult to be interpreted by an intruder or attacker. At the end of the communication, the recipient can decrypt the original message using the secret key.

It is observed that the GUI is very much worth in encryption of messages and testing the validation of the developed ciphers within minimum possible time. In future more number of developed ciphers and cryptanalytic procedures can be incorporated. This GUI can be used in universities and research centers as a tool for studying chaotic cryptography.

10. REFERENCES

[1] Jakimoski G. and Kocarev L., 2001, "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps," IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, 48(2), 163–169.

[2] Dachselt F. and Schwarz W., 2001, "Chaos and cryptography," IEEE Trans. Circuits and Syst. I, 48(6), 1498–1509.

[3] Oliveira de L. P. and Sobottka M., 2008"Cryptography with chaotic mixing," Chaos, Solutions and Fractals, 35(3), 466–471.

[4] Anstett F., Millerioux G., and Bloch G., 2005, "Message-embedded cryp¬tosystems: Cryptanalysis and identifiability," in Proc. 44th IEEE Conf. Decision and Control, 44(3) ,2548-2553.

[5] Xiang T., Wang S., H. L, and Hu G., 2007 "A novel symmetrical cryptosystem based on discretized two-dimensional chaotic map," Physics Letters A, 364(3-4), 252–258.

[6] Alvarez G. and Li S., 2006 "Some basic cryptographic requirements for chaos-based cryptosystems," Int. J. Bifurc. Chaos, 16(8), 2129-2151.

[7] Ruming Yin, Jian Yuan, Qiuhua Yang, Xiuming Shan, Xiqin Wang, 2009," Linear cryptanalysis for a chaos-based stream cipher," World Academy of Science, Engineering and Technology ,60, 799-804.

[8] Jiantao Zho, Au, O.C, 2010, "Cryptanalysis of chaotic convolutional coder ", Proceedings of IEEE Symposium Circuits and Systems (ISCAS) , 145-148.

[9] S. Li, X. Zheng, 2010, "Cryptanalysis of a chaotic image encryption method", Proceedings of the IEEE International. Symposium on circuits and systems, Scottsdale, AZ, USA.

[10] P. Xu; J. Zhao; D. Wang, 2011, "A selective image encryption algorithm based on hyper-chaos", IEEE 3rd International Conference on Communication Software and Networks (ICCSN), 2011, 376-379.

[11] Mina Mishra, Dr. V.H.Mankar, 2011, "Chaotic Encryption Scheme Using 1-D Chaotic Map" Int. J. Communications, Network and System Sciences, 4, 452-455.

[12] Mina Mishra, Dr. V.H.Mankar, 2011,"Review on Chaotic Sequences Based Cryptography and Cryptanalysis" International Journal of Electronics Engineering (IJEE), 3 (2), 189– 194.

[13] Mina Mishra, Dr. V.H.Mankar, 2012, "A Chaotic encryption algorithm: Robustness against Brute-force attack" Advanced Intelligent and soft computing (AISC), Springer, 167, 169-179.

[14] Mina Mishra, Dr. V.H.Mankar, 2012, "Chaotic Cipher Using Arnolds and Duffings Map" Advanced Intelligent and soft computing (AISC), Springer, 167, 529-539.

[15] Mina Mishra, Dr. V.H.Mankar, 2012, "Design and Analysis of Cipher Based on Henon And Burger Maps" Proceedings of IEEE 4th International Conference on Electronics Computer Technology (ICECT- 2012), 978-1-4673-1850, 466-471.

♦♦♦