JOURNAL OF THEORETICAL PHYSICS & CRYPTOGRAPHY

www.IJTPC.org/Publications

CRYPTANALYSIS OF CHAOTIC CIPHER BASED ON IDENTIFIABILITY CONCEPT

Mina Mishra[1], V.H. Mankar[2]

Department of Electronics & Telecommunication, Nagpur University, Nagpur Maharashtra, India[1]

Department of Electronics Engineering, Government Polytechnic, Nagpur Maharashtra, India [2]

ABSTRACT

Cryptanalysis of chaotic ciphers based on concept of identifiability is presented and discussed in this paper. Both the ciphers are developed using 2-D chaotic map and parameter of map acts as secret key. The ciphers are developed using Henon and Burger map. Key space analysis of cipher provides the range of keys. The keys are then selected randomly from domain of key space and they are tested for identifiability. Identifiability concept of cryptanalysis is accompanied with other basic cryptanalytic procedures like avalanche effect. Analysis of keys has been accomplished on various texts. It is concluded that identifiability concept of testing the strength of chaotic ciphers, against brute force attack in prior to sending message, proves to be quite advantageous. The developed ciphers are found to have identifiable key and good key sensitivity which concludes that they can resist linear and brute force attacks.

Keywords

Cryptanalysis, 2-D Chaotic map, Identifiability, Avalanche effect.

1. INTRODUCTION

Chaotic signals are broadband, noise like and difficult to predict. Many researchers used chaotic systems for information masking[3]. The proposed communication schemes involve a chaotic transmitter system and a receiver system. The transmitter input is the information to be masked, the plaintext, and its output is the encrypted information, the cipher text, conveyed to the receiver. Several methods for “hiding” an information signal into a chaotic signal have been proposed in the literature [1], [2].

According to the chronology in [6], [8] an overview can be observed including the chaotic masking, the chaotic switching, the parameter modulation, the message embedding. These methods are defined either for continuous-time or discrete-time systems. In general, the decryption mechanism requires the synchronization between the transmitter and the receiver. An essential issue for the validation of cryptosystems is the cryptanalysis, that is the study of attacks against cryptographic. A fundamental assumption in cryptanalysis, first stated by A. Kerkhoff in 1883 [8], is that the adversary knows all the details of the cryptosystem, including the algorithm and its implementation, except the secret key, on which the security of the cryptosystem must be entirely based. As for chaotic cryptosystems, the system parameters play an important role as they act as the secret key.

Parameters recovering [9] is one of the problems of great importance related to this issue. It is shown that the considered encryption schemes are not sufficiently sensitive to parameter mismatch. In fact, synchronization for decryption can be achieved despite the parameter mismatch. This reduces the set of all possible key values and reducing this key space increases the chance for the adversary to find the actual key value. “Error function attack” proposed in one of the literature [10] consists in trying a key in the reduced key space and in computing the difference between the output of the actual system and the output of the candidate system, both of them being forced by the same plaintext. If the difference converges to zero, the actual key is recovered. The reconstruction of the system parameters can be refined by resorting to adaptive techniques. The basic idea is to adaptively adjust the parameters to achieve synchronization with remote chaotic systems. A somewhat different method can be found in [7], where a chosen cipher text attack is considered. For such an attack, the adversary is assumed to control the input of the receiver, the cipher text, and to analyze the corresponding plaintext sequence. It is shown that the parameters can be reconstructed by solving a set of

algebraic equations. All these works deal with some identification techniques [4], [5] for reconstructing the parameters and most often on some special cases.

In this paper, Cryptanalysis of chaotic ciphers based on concept of identifiability is presented and discussed. Both the ciphers are developed using 2-D chaotic map and parameter of map acts as secret key. The ciphers are developed using Henon and Burger map. Key space analysis of cipher provides the range of keys. The keys are then selected randomly from domain of key space and they are tested for identifiability. Identifiability concept of cryptanalysis is accompanied with other basic cryptanalytic procedures like avalanche effect. Analysis of keys has been accomplished on various texts.

The rest of the paper is organized as follows. Section II, discusses the methodology involved during encryption in both the ciphers. Section III, presents cryptanalytic procedures developed and followed to perform on the ciphers. Section IV presents the analysis result in tabulated form and discussions. Section V concludes the work.

2. METHODOLOGY

This section discusses about the methodology involved in designing of both ciphers.

(A) Message-Embedded Scheme

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

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

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 $\theta, \theta = [\theta^{(1)}, ..., \theta^{(L)}]^T \in \Theta \subset R^L$, the parameter vector? The most common nonlinearities f_θ are of polynomial type (Henon map, Logistic map, Burger map, ...), $[m_k]$ means that h_θ can depend on m_k but not necessary.

3. CRYPTANALYSIS

Some of the basic cryptanalytic procedures taken from cited paper are developed to analyze the designed ciphers. They are discussed in descriptive manner 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. 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:

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 $\theta \in v(\theta)$

$$\hat{\theta} \neq \theta \Rightarrow \{y_k(x_0, m_k, \hat{\theta})\}_0^T \neq \{y_k(x_0, m_k, \theta)\}_0^T \quad \text{...(2)}$$

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 following, it can be equally said that the system or its parameters are structurally identifiable.

In the definitions above, the subset X_0 is open in order to avoid considering an atypical 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, any time step k can be considered because the system (1) is shift-invariant.

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

Output 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

$$\{y_k(x_0, m_k, \hat{\theta})\}_0^T = \{y_k(x_0, m_k, \theta)\}_0^T \quad \text{... (3)}$$

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 (5) $\Rightarrow \hat{\theta} = \theta$. 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.

Output Equality Approach: 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).

4. ANALYSIS RESULT

Keys have been selected randomly from the domain of key space of each cipher and they are tested for their validity against most basic attacks.

(A) Cipher I:

This cipher is developed by embedding message in Henon chaotic map. Key space of this cipher ranges from [-0.9 2.19 -0.44 0] to [1.39 2.22 -0.45 0.277]. From table I, it can be observed that plaintext sensitivity ranges from 0.3% to 2% and key sensitivity ranges from 7 % to 20 %. Conclusion about the identifiability of the all chosen key is derived for the given specifications.

TABLE 1: ANALYSIS OF CIPHER I

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	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	YES
2.	Meet me after 5p.m.	[-0.85 2.19 -0.35 0.1]	□_ 4□□ o□¤ X□¤ X□³ □□_ 4□¬ 5□¤ X□_ 4□ c□¥ U□³ □□¤ X□± □□_ 4□t U□¯ !□m K□¬ 5□m K	0.8750	14.8750	[-0.85 2.19 -0.35 0.1] to [-0.795 2.195 -0.35 0.1]	I	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	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□« Â□n U	0.8333	13.5714	[-0.75 2.2 - 0.35 0.15] to [-0.645 2.205 - 0.35 0.15]	I	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	YES
6.	How to do analysis?	[0 2.2 - 0.35 0.2]	□b □□□Y $□±□□1□¹□ 4 □b □□¶□□3□±□□1 □b□□¦ □- □±□□1□b	0.75	20.6250	[0 2.2 -0.35 0.2] to [0 2.205 -0.35 0.2]	I	YES

			£}, ± 1 £}, - 0 » 4 µ 2 « / µ 2 L !					
7.	Hai! Where are you going?	[1.1 2.22 -0.45 0.2]	g ©Ö © ± h µ g ©Ö Ž - ¹ - g ©Ö © ¹ - g ©Ö À · ¼ g ©Ö - · ± µ -	1.25	11.25	[1.1 2.22 -0.45 0.2] to [1.105 2.22 -0.345 0.2]	I	YES
8.	Dolly, are you coming with me?	[1.2 2.1 -0.45 0.1]	d ² ³ ° ° ½ p¹ d ² ¥ ¶ © d ² ½ ³ ¹ d ² § ³ ± - ² « d ² » - ¬ d ² ± ©	0.4032	10.5645	[1.2 2.1 -0.45 0.1] to [1.205 2.105 -0.45 0.1]	I	YES
9.	Children are playing in park.	[1.2 2.1 -0.45 0.12]	d ¸ ¬ - ° ¨ ¶ © ² d ¸ ¥ ¶ © d ¸ ´ ° ¥ ½ - ² « d ¸ - ² d ¸ ´ ¥ ¶ - rÃ d ¸	0.8065	10.0806	[1.2 2.1 -0.45 0.12] to [1.2 2.105 -0.345 0.12]	I	YES
10.	I shall go to cinema.	[1.3 2.2 -0.44 0.22]	h§ h§ » ° © ´ ´ h§ - · h§ ¼ · h§ « ± ¶ - µ © vä	0.3409	7.0455	[1.3 2.2 -0.44 0.22] to [1.305 2.205 -0.44 0.22]	I	YES

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

(B) Cipher II:

In this example of cipher message is embedded in Burger map. Table II concludes that key space is from [0.77 0.83] to [0.9 1.17] i.e., $4x10^{12}$, Plaintext sensitivity ranges from 0.4% to 1.9% and key sensitivity ranges from 0 % to 28%. Conclusions about the identifiability of the chosen key is derived for the given specifications for particular keys.

TABLE 2: ANALYSIS OF CIPHER II

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	Whether key can act as secret key against Brute Force attack?
1.	How are you?	[0.71 0.84]	l »ÃI-¾±lÅ» Á	0.9615	24.0385	[0.71 0.84] to [0.715 0.841]	I	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	NO
3.	I have a gift for you.	[0.73 0.86]	k k³¬Á°k¬k² ´±¿k±º½kÄº Ày	1.6304	26.0870	[0.73 0.86] to [0.732 0.865]	I	YES
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	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	NO
6.	How to do analysis?	[0.76 0.89]	l »ÃlÀ»l°»l- º-¸Å¿µ¿	0.6250	27.5000	[0.76 0.89] to [0.765 0.89]	NI	NO
7.	Hai! Where are you going?	[0.77 0.9]	m ®¶nm¤µ ²¿²m®¿²mÆ ¼Âm´¼¶»´	0.9615	23.0769	[0.77 0.9] to [0.775 0.9]	NI	NO
8.	Dolly, are you coming with me?	[0.771 0.83]	k º··Äwk¬½ °kÄºÀk®º¸´¹² kÂ´¿³k¸°	1.2097	0	[0.771 0.83] to [0.776 0.832]	NI	NO
9.	Children are playing in park.	[0.772 0.831]	j ²³¶®¼¯¸j« ¼¯j º¶«Ã³¸±j ³¸jº«¼µxj	0.4032	22.5806	[0.772 0.831] to [0.777 0.832]	NI	NO
10.	I shall go to cinema.	[0.773 0.832]	k k¾³¬··k²º k¿ºk®´¹º¸¬y	1.7045	0	[0.773 0.832] to [0.778 0.833]	NI	NO

5. CONCLUSION

In this paper, cryptanalysis of chaotic cipher based on identifiability concept is discussed and presented. Both the ciphers are developed using 2-D chaotic map and parameter of map acts as secret key. The ciphers are developed using Henon and Burger map. Key space analysis of cipher provides the range of keys. The keys are then selected randomly from domain of key space and they are tested for identifiability. Identifiability concept of cryptanalysis is accompanied with other basic cryptanalytic procedures like avalanche effect. Analysis of keys has been accomplished on various texts. Identifiability is a systematic methodology to test, a priori, during the design stage, whether the parameters of a chaotic cryptosystem may play the role of the secret key or not. From a cryptanalysis point of view, this paper leads to the following conclusions. Firstly, if the parameter vector of the transmitter is identifiable, it is more difficult for the eavesdropper to find it by a brute force attack (exhaustive search). Consequently, this parameter vector may be a good candidate to play the role of the secret key against a brute force attack. If the parameter vector is not identifiable, the eavesdropper has a higher favorable chance to find it by a brute force attack. Thus, this parameter vector is a bad candidate to play the role of the secret key against a brute force attack. Secondly, if the parameters are identifiable, which is a necessary condition for the security against brute force attack, obviously not sufficient since sensitivity or specific statistical properties are also required, an explicit form of each parameter can be established.

The developed ciphers are found to have identifiable key and good key sensitivity which concludes that they can resist linear and brute force attacks.

A comparison table III shows that both ciphers are found to resist brute-force attack as they consist of identifiable keys.

TABLE 3: COMPARISON BETWEEN THE TWO CIPHERS

Name of Cipher	key Space	Range of plaintext sensitivity	Range of key sensitivity	Identifiable key	Whether key space > 2^{100}
Cipher I	$9x10^{28}$	0.4 to 2 %	9 to 20 %	Yes	No
Cipher II	$4x10^{12}$	0.4 to 1.9 %	0 to 28 %	Yes	No

6. REFERENCES

[1] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," Int. J. Bifurc. Chaos, 2006.

[2] G. Millérioux, A. Hernandez, and J. Amigó, "Conventional cryptography and message-embedding," in Proc. 2005 Int. Symp. Nonlinear Theory and its Applications (NOLTA 2005), Bruges, Belgium, Oct. 18–21, 2005.

[3] H. Delfs and H. Knebl, Introduction to Cryptography. Berlin, Germany: Springer-Verlag, 2002.

[4] 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.

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

[6] M. J. Ogorzalek, "Taming chaos – Part I: Synchronization," IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol. 40, no. 10, pp. 693–699, Oct. 1993.

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

[8] T. L. Carroll and L. M. Pecora, "Synchronizing chaotic circuits," IEEE Trans. Circuits Syst., vol. 38, no. 4, pp. 453–456, Apr. 1991.

[9] T. Yang, "A survey of chaotic secure communication systems," Int. J. Comput. Cogn., vol. 2, no. 2, pp. 81–130, 2004.

[10] X. Wang, M. Zhan, and C. H. Lai, "Error function attack of chaos synchronization based encryption schemes," Chaos, vol. 14, no. 1, pp. 128–137, 2004.