Journal Engineering Sciences
& Information Technology
Issue (2), Volume (3)
June 2019
ISSN: 2522-3321

المجلة العربية للعلوم و نشر الأبحاث
Arab Journal of Sciences & Research Publishing
AJSRP

Black Box Attack of Simulation Secret Key using Neural-Identifier

Khaled M. Alalayah **Khadija M. H. Alaidarous**

Ibrahim M. G. Alwayle **Ahmed A. Alattab**

Faculty of Science and Arts || Sharurah, Najran University || KSA

Abstract: The issue of the cryptanalysis is defined as the unknown issue or problem related to the identification of the system where the major goal of the cryptanalysis is for the design of the system for various steps involved. Neural networks will be ideal tool for Black-Box system identification. The black-Box attacks against secret key cryptosystems (stream cipher system) would be presented by considering a Black-Box Neuro-Identifier model to retain two different objectives: first is for finding out the key from the provided plaintext-cipher to pair, while the second objective is to emulator construction a neuro-model for the target cipher system. There are many researches going on considering the various models of encryption where ANN is being used as single layered or multi layered perceptron. The above defined cryptographic techniques are sometimes also termed as the Neural Cryptography. As the ANN model relies on the feedforward working criteria means it can be used for the generation of some effective and efficient encryption methodologies. Cryptanalysis is considered as significant footstep for evaluating and checking quality of any cryptosystem. A portion of these cryptosystem guarantees secrecy and security of huge data trade from source to goal utilizing symmetric key cryptography. The cryptanalyst researches the quality and distinguishes the shortcoming of the key just as enciphering calculation. With the expansion in key size, the time and exertion required anticipating the right key increments. These systems for cryptanalysis are changing radically to decrease cryptographic multifaceted nature. In this paper a point by point study has been directed. Much cryptography strategies are accessible which depend on number hypothesis however it has the hindrance of necessity a substantial computational power, unpredictability and time utilization. To defeat these disadvantages, artificial neural networks (ANNs) have been connected to take care of numerous issues. The ANNs have numerous qualities, for example, learning, speculation, less information necessity, quick calculation, simplicity of usage, and programming and equipment accessibility, which make it exceptionally alluring for some applications. This paper gives a cutting-edge survey on the utilization of counterfeit neural systems in cryptography and concentrates their execution on estimation issues identified with cryptography.

Keywords: Cryptanalysis, Encryption, Ciphertext, Plaintext, ANN.

هجوم الصندوق الأسود لمحاكاة أنظمة التشفير الانسيابي باستخدام المعرف العصبي

خالد محمد العلاية **خديجة محمد العيدروس** **إبراهيم محمد الوايلي** **أحمد عبدة العطاب**

كلية العلوم والآداب || شرورة || جامعة نجران || المملكة العربية السعودية

الملخص: تُعرّف قضية تحليل الشفرات بأنها المشكلة أو المشكلة غير المعروفة المتعلقة بتحديد النظام حيث الهدف الرئيسي من تحليل الشفرات هو تصميم النظام لمختلف الخطوات المتضمنة. الشبكات العصبية ستكون أداة مثالية لتحديد نظام Black-Box. سيتم تقديم هجمات الصندوق الأسود ضد أنظمة التشفير السرية الرئيسية (نظام التشفير المتدفق) من خلال الأخذ بعين الاعتبار نموذج معرّف عصبي الصندوق الأسود (Black-Box Neuro-Identifier) للحفاظ على هدفين مختلفين: الأول هو اكتشاف المفتاح من شفرة النص العادي المقدمة إلى زوج، في حين الهدف الثاني هو محاكي بناء نموذج عصبي لنظام التشفير المستهدف. هناك العديد من الأبحاث الجارية في ضوء النماذج المختلفة للتشفير حيث يتم استخدام ANN كطبقة أحادية الطبقة أو متعددة الطبقات. أحيانًا ما تُعرف أيضًا تقنيات التشفير المحددة أعلاه باسم "التشفير العصبي". ونظرًا لأن نموذج ANN يعتمد على معايير العمل المتطورة، فيمكن استخدامه في توليد بعض منهجيات التشفير الفعالة والفعالة. ويعتبر Cryptanalysis بمثابة خطوة مهمة لتقييم وفحص جودة أي نظام تشفير. ويضمن جزء من نظام التشفير هذا السرية وأمان تجارة البيانات الضخمة من المصدر إلى الهدف باستخدام تشفير المفتاح المتماثل. يبحث cryptanalyst الجودة ويميز القصور من المفتاح فقط كما تشفير الحساب. مع التوسع في حجم المفتاح، يتطلب الوقت والجهد توقع الزيادات الرئيسية الصحيحة. هذه الأنظمة لتحليل الشفرات تتغير جذريًا لتقليل الطبيعة متعددة الأعمدة المشفرة. في هذه الورقة تم توجيه دراسة نقطة. يمكن الوصول إلى الكثير من استراتيجيات التشفير التي تعتمد على فرضية الأعداد، ومع ذلك فإنها تعيق الحاجة إلى قوة حسابية كبيرة، وعدم القدرة على التنبؤ واستخدام الوقت. لهزيمة هذه العيوب، تم ربط الشبكات العصبية الاصطناعية (ANNs) بالعناية بالعديد من القضايا. تمتلك ANNs العديد من الصفات، على سبيل المثال، التعلم، والمضاربة، وأقل الحاجة إلى المعلومات، والحساب السريع، وبساطة الاستخدام، والبرمجة والوصول إلى المعدات، مما يجعلها مغرية بشكل استثنائي لبعض التطبيقات. تقدم هذه الورقة مسحًا متطورًا حول استخدام الأنظمة العصبية المزيفة في التشفير وتركز تنفيذها على مشكلات التقدير المحددة مع التشفير.

الكلمات المفتاحية: تحليل الشفرة – التشفير – النص المشفر – النص الصريح – الشبكات العصبية الاصطناعية.

I. Introduction

As defined in literal and scientific texts, cryptology is the art and science of designing and analysing algorithms that serve as primitives to establish information security goals such as confidentiality, integrity, authentication and non-repudiation in different information systems deployed in various application environments. These goals will be discussed in details subsequently in this chapter [10]. In a view of the previous definition, cryptology has always been mapped to two main lines of study cryptography and cryptanalysis.

Today, cryptography can be finely defined as the aspect of the mathematical design and implementation of the fundamental components that will maintain information security goals within certain cryptographic and security margins. These fundamental components are described as cryptographic primitives. The other face of the coin is cryptanalysis which is defined as the art and science related to evaluating, verifying and testing the designed cryptographic primitives and pushing them through all possible claimed or non-claimed security margins[14]. The exact definition of these security and cryptographic margins will follow within this text.

II. BACKGROUNDFOR CRYPTANALYSIS

In the general format the data mining is being used for the purpose of extraction of the data which can be for the usage of the individual level, for business particulars and many more. Shaligram and R.S. Thakur in 2013[5], firstly considered the term "Cryptic Mining", for the domains having low level of data. The cryptic Mining is being generally being used for providing better security to the system and also is helpful for the hackers and cryptanalytics to strengthen the security level of the cryptosystem. Figure 1 depicts the Various Approaches towards Cryptanalysis (AVK) based cryptosystem where the concept of cryptic mining is being used.

The techniques of cryptic mining are being used for the traditional techniques of data mining, where the patterns and key size detection is being done which also being used for strengthen the methodology. As, at the time when the cipher is being generated it is just random text which is quite difficult in practice to consider the same. At the time of generation of the cipher text and plain text for input it is possible that the generation may follow some specific patterns. The cryptic mining methodology can be used harness the weaknesses of the process as the patterns followed while the generation are somewhere available over the storage segment or over the internet which can be used to exploit the security of the system.

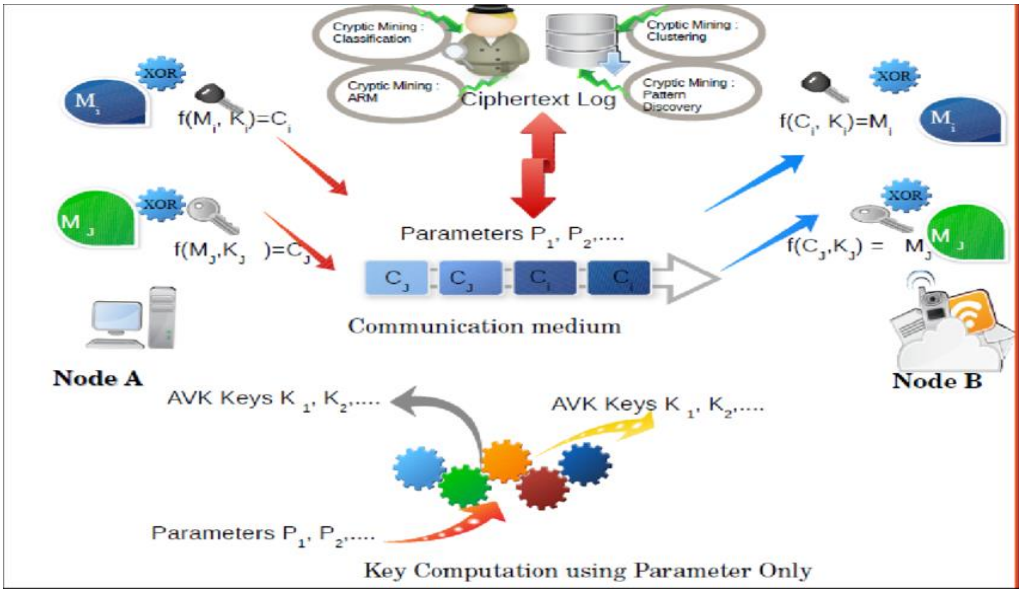

Figure (1) A framework for Cryptosystem and Cryptic Mining with AVK

Approaches towards Cryptanalysis

- **Classification:** It is being used for the detection of the scanners of the cipher text for deciding the nature and also for deciding the class of the algorithm.

- **Clustering:** The ciphertext is being clustered into groups on the basis of some similarity criteria for the better prediction and pattern discovery of the methodology.
- **Association Rule:** These set of algorithm investigates rules for associating parameters based relationships together with (plain-text, cipher-text) paired associations [1].
- **Pattern discovery:** In these methodologies the sets are being made available as input which actually works as scanners in the high-end analysis tools like Markov model [2], ANN, GA, ACO etc. The methodologies can also be used for the detection of the nature and behavior of the different types of malwares and also for the analysis of the ad-wares, also different classes of attacks for which the honey-pot and honey-net system is being utilized.

III. GOALS OF A CRYPTANALYST

For an exploitation on a cryptosystem to be qualified as an attack, it should provide a potential practical feasibility less than brute force. It should be clarified that the general goal of a cryptanalyst or an attacker is to recover the secret key of the cryptosystem. However, in some cryptosystems this is not always achievable which introduce an alternative taxonomy of attacks based on the goals, achieved results and obtained information by an attacker [3]. They can be listed as the following ordered from the strongest to the weakest:

- **Total Break:** The attacker achieves the goal of retrieving the key of the user or the secret key used in the cryptosystem. It is alternatively referred to as key recovery attacks. This type of attack might need a high data complexity as in a large number of plaintext/ciphertext pairs. Brute force is considered a possible type of key recovery attacks. If a few pairs of plaintext/ciphertext was given along with the size of the key for certain block cipher[4].
- **Global Deduction:** The attacker will be able to obtain an equivalent algorithm for encryption or decryption without further knowledge on the key[4].
- **Local Deduction:** The attack will be able to generate the ciphertext to a given plaintext, or plaintext to certain ciphertext. This can translate to state recovery in stream ciphers where an internal state can be recovered given partial keystream and additional public information[4].
- **Distinguishing Algorithm:** The attacker has access to a black box of the cryptosystem. He/she can distinguish between block cipher using a randomly cho- sen secret key, and randomly selected permutation. For example, this can be achieved also through formal statistical hypothesis testing as Neyman-Pearson paradigm [4].

IV. CRYPTIC CLASSIFICATION USING ANN

ANN is very much similar to human brain for which two different aspects are being considered as under:

1- The ANN system considers the knowledge acquiring by a specific learning process.

2- The knowledge acquired from the environment and also from the learning process which is also known as the synaptic weights is stored in the intermediate nodes. The complex patterns and problems can also be done easily using the ANN methodology where the complexity considered is either from humans' side or using the computer machine.

Other advantages include:

1- **Adaptive learning:** ANN is capable for considering the process on the basis of training data which is provided for the learning process or some previous generated data.

2- **Self-Organization:** The data or the information which is being acquired during the learning process can be represented in the any of the specific way as described in the process.

3- **Real Time Operation:** Parallel computation is possible in the ANN based techniques for which some specific hardware's are used to take full advantage of the abilities of the ANN.

Three types of algorithms are used in cryptography in ANN:

a. Secret Key Cryptography
b. Public Key Encryption
c. Hash Functions

[5] The technique allows the cryptanalysts to make use of the advanced tools which can be better used for the detection of the weaknesses of the cryptosystem. In the case when the polynomial time frame is being considered then the extraction of the hints about the original information for the large corpus. Corpus generally are the large texts and these are generally considered by cryptanalysts with large databases where the corpus is having large number of cipher and plain text patterns and also hash files. At the time when the patterns or cipher text are stored in the datasets then it are generally being mixed up with the already stored and are generated by the other available schemes and methodologies where the key size is varied, different protocols, types of ciphers generation algorithm, degree of exposures of information about key space and many other information related to plaintext, ciphertext, relationship between them. The stored data in the datasets may be cropped or shorted using the newly generated techniques. The figure 2 shows similar type of work for shorting or grouping of the data stored in the dataset. The developed technique considers three following parameters as the properties of the cipher text as x, y and z. In the case when the key is being considered with parameter -1 then the outcome for the same will be 1 else will be -1.

With respect to the next parameter y the scanner will return 1 if it through y. In the same way the sensor technique will work for the third parameter z. The three outcomes of the sensor technique will act as input to the neural network also termed as classifier, where the classifier is being used to decide the type of cipher in the dataset for grouping it to the correct cluster. Considering an example of two different such classes as class-1(For AES: C_1, C_3,C_4) and class-2(For DES C_2,C_5). Just because of the classification of the class there are only two types of clusters present in the log of the dataset. The cipher which passes from the sensor algorithm can be represented in 3-D vector having parameter set P = [x y z] .

The output prototype for class-1 is [1 -1 -1] and output for class-2 will be [1 1 -1].

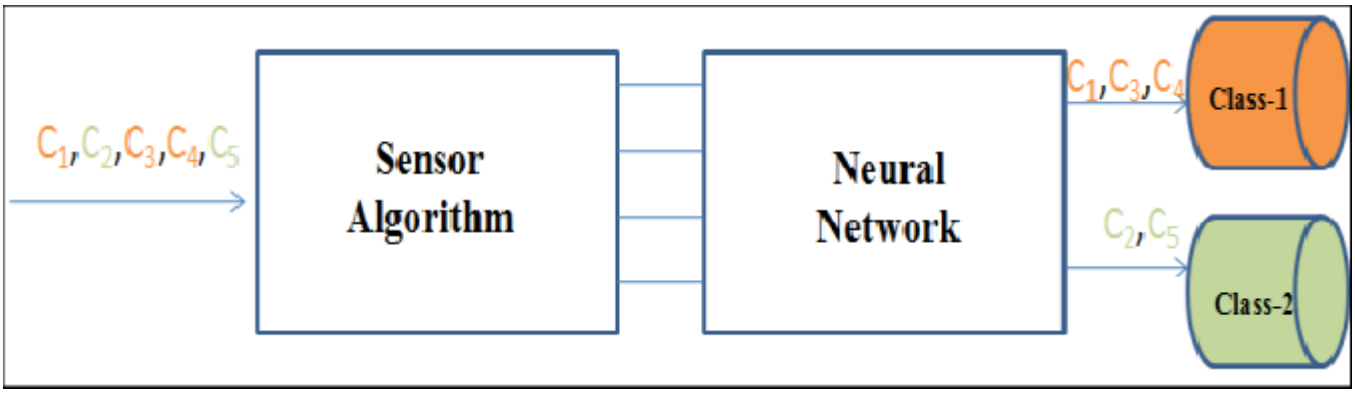

Figure (2) ANN model fop Classifier for cryptanalysis

For the every of the log captured the ANN will consider a 3-D input which is being used for classifying the cipher as class-1 or class-2. For the depiction to solve such type of situations single layered perceptron can be used. In the case when the outcome is 1 then the cipher text of type class-1 is provided as input and the outcome is -1 in the case when the cipher text is of type class-2.

V. SOME CRYPTANALYSIS TECHNIUQES

Wolfgang Kinzel in his work considered the secret key with ANN for the public channel. The considered technique have two multi-layered perceptron's are considered where the inputs for training are the output bits which are enabled for synchronization. The considered two networks are having some of the initial weights where they share there data to be used for training where the considered synaptic weights are time dependent variables. None of the two-perceptron used share any of the information over the channel before the communication starts. The process of the synchronization is being considered as the step for key generation in the ANN [14]. The secret key for the process of encryption can be the similar weights of the two available networks. The public which are not the part of number theory, the neural cryptography is being used for key generation. On the basis of the results it can stated that the methodology is quite simple, fast and secure [6].

Einat Klein in his work proposed cryptographic technique where the secret key is based on the ANN for the public channels. The algorithm considers two different network for which the equally time dependent weights are considered as the training data via chaos synchronization system where the initial conditions are different for both the networks. The logistic chaotic map is being used for the integration of both the networks.

The available neural networks are considered as the input for the partners for the logistic maps where the output bits are generated as to be learned. The two available network mutually communicates with one another and generates matching signal for chaotic maps. The usage of the chaotic maps actually have enhanced the security in the cryptographic system specially talking about the neural based cryptography [7].

N. Prabakaran in his work proposed a methodology for the secret key generation using the neural cryptography where author has used the Tree parity machine (TPMs) using the concept of mutual learning. The system is having two separate systems having two different initial conditions and are being synchronized by two common inputs where the inputs are being coupled for two different systems. Right after the computation of the outcomes the two available network get the common vector as input and the weights are updated on the basis of the mutual outcomes on every of the stages. The relations between the input and the outcomes are not shared over the public channel till the weight vectors are found matching and are like to be used as the secret key for process of encryption and decryption for the message to be transmitted. Random numbers are used as input vector for two networks where the vectors are generated using the Pseudo-Random Number Generators (PRNGs). The proposed model fixed the security against numerical attacks [8].

R. M. Jogdand in his work considered a common secret key which actually relies on the neural cryptography. The neural cryptography is having two networks for communication where the input vectors used as input and the networks are being trained on the basis of provided vectors. The networks are initiated by the random weights and where the object weights are generated by different source and the exchange of the final outcome bits is done after generation of the output bits among different patterns. The outcome bits may be modified in the case when the bits are same for both the partner networks. The weights which are updated act as secret key for the process of encryption and decryption. On the basis of the presented results it can be stated that the neural based cryptosystems are quite secured [9].

Pratap Singh also proposed a technique of secret key generation in his work for the public channel. The methodology considers two networks where the networks are initiated and both the networks are having differing conditions where the weights are synchronized with the help of some external signals and received a common random input vector and learned their mutual output bits.

The synaptic weights available with the networks are considered as the secret key in the public channel. The results and discussion stated by the author represents that the things are quite secure and efficient too [10].

Differential cryptanalysis attacks are being defined as the plaintext selected by the user where it is also being considered as the most preferable tool by the researchers as it can be used for attaining the desired results considering the differentiating primitives. The facts were later on discussed by the author in [11] which was then published in the research by Biham and Shamir in [12]. In the work the difference between the input and output is being considered using the structure of the cipher text, for a specific number of rounds, and detect the non-random behaviour exhibited in the final output, with a certain probability usually high. It is considered to be a much effective alternative to considering the values of a plaintext and its corresponding ciphertext. These difference are utilized through an XOR operation in general, yet it is potentially applicable to use arbitrary group operations, modular addition (i.e as in IDEA and SAFER) or Unsigned Non-Adjacent Forms (UNAF) as in ARX structures to indicate these differences. The differential property can be utilized to re- cover the parts of the subkeys, typically the first or the last, in a reduced r-round version of the cipher, or alternatively deduce information about the secret key. r indicates the number of rounds under study.

Integral attacks were first introduced by Knudsen in their application on SQUARE and later on was applied and generalized under different references as in multiset attacks and saturation attacks on Two fish [13]. The attack relies on constructing sets of or multisets of chosen plaintexts that either sum to a constant or differs in certain parts of the set. Thus exploiting relations between various encryptions. The main goal of the attack is to follow the preservable nature of certain properties of the sets. For example, in integral attacks, the set I of internal states are constructed such that they differ in only one-byte d_0 which covers all 2^8possibilities. It is noted that this property will hold after an application of an S-box layer (or a bijective transformation) to the state I. While the diffusion layer will make the rest of the bytes active [14].

VI. CRYPTOSYSTEM AND IOT

Currently IOT is also increasing stride, here device and Internet is linked to the real world via ubiquitous sensors". The theory of communication among devices is not a novel phenomenon. Currently, communications between devices also have been established with automated devices. Organization of IoT technology is challenging more intellect, more complication – into the conversation. With the development of Computational Intelligence approach, Intelligent Agent Based System seems to be the support and need of upcoming scientific era that are proficient to offer intellectual Device-to-Device communication and IoT connection resolutions for wired and wireless systems for the welfares of organization and Society.

Meanwhile light-weight cryptography, methodologies are mandate of present and as well as upcoming systems. To enhance security AES, DES, RC4, Blowfish, TwoFish etc algorithms are used. The Newest style in symmetric cryptography is to expansion of key size, which tends to advanced control and calculation period. We still do not have better candidate in Hash and symmetric key encryption function. In this paper, we highlight the effectual method of improving them to be prepared for novel scopes of IOT. Fibonacci-Q, Sparse approach and cryptic-mining are aligned in the extension of AVK concepts, with hacker's and cryptanalyst perspectives are discussed in our work.

Following research questions are yet to be answered:

1- What are the possibilities of AVK methods of confirming efficacy in IOT? Particularly when heterogeneity is extreme like for systems with connectivity at the "edge" of nets in distant and challenging situations, using Ethernet, serial, USB and wireless connections.
2- How device would preserve reliability on functioning over WSN?
3- How device will regulate and direct keys in g IoT atmospheres?
4- How system will be considered to work strongly on organizing intellect at the network edge? The work also unlocks a different way to consider about effectual security procedure for conversation machines in IOT atmosphere using AVK and makes the sources for AVK centered security architectures with the subjects of key organization system, comprising key provisioning, key revising policy or key agreement.

VII.DISCUSSION

In this paper, many of the important ANN techniques have been presented and analyzed. These techniques are based on:

- The Tree Parity Machines (TPM) was used to generate a secret key over the public channel on the output at each partner.
- The neural network with chaotic logistic map was used for cryptography by which both partners use the neural network as input for the logistic map, that generate the output bits to be learned.
- The General Regression Neural Network (GRNN) was used for encryption and decryption process based on three layers, where the input data divided into 3 bits and 8 bits as output.
- The training back-propagation neural network was act as public key, while Boolean algebra act as private key.
- The chaotic Hopfield neural network with time varying delay was used to generate binary sequence for making plaintext, which considered as a random switching function for chaotic map.

- The neural network based on chaotic generator was used for generate chaotic dynamic act as a shard key.
- The initial weight value of the neural network was used after training as symmetric key.
- The Pseudo Random Number Generator (PRN) based on neural network was used in stream cipher as a key sequence generator.
- The chaotic neural network was used to generate chaotic sequence act as a triple key (combined of initial condition and control parameters) for cryptography.
- The Layer Recurrent Neural Network (LRNN) was used to generate pseudo random number based on weight matrix obtained from layer weight of the LRNN.

Table (1) Cryptic Mining: Some Classification approaches.

No.	Method	Concept	Features	Limitations
1.	Rule-based Classifier	If...then ... like rules	Simple to Use	Complex situation are hard to define in Simple rules
2.	Bayesian Networks	Probability of patterns in ciphers or key	Efficient with causal relations	Cannot handle missing data well
3.	Artificial Neural Network	Mathematical model calculating output based on inputs	Can handle complex relations	Black box
4.	Support Vector Machines (SVM)	Classes of ciphers are separated by a hyper plane by calculating support vectors to the closest points from each class	Small chance at over fitting and possible to use dynamically	Slow on large sample sizes
5.	Decision Trees	Classification by If..then..like tree structure	Can handle numeric and text data types	Very hard to find optimal solution

Table (2) Cryptic Mining: Some Classification approaches.

No.	Method	Concept	Features	Limitation
1.	KNN	Distance/ density computation between objects and classes.	Simple to implement	Storage intensive and susceptible to noise

No.	Method	Concept	Features	Limitation
2.	HMM	The probability of a sequence of observed encrypted objects is used to calculate the probability of a sequence of non-visible events.	Can analyze sequences of events in which the events are not independent	Events must be independent. (The events may not provide a probability of a event.)
3.	k-means	Clustering based on equality Clusters data into a Given number of k clusters by minimizing the mean	Insensitive to noise and cluster shape Pre-classification not necessary	Initial choice of parameter values Hard to find Optimal solution and sensitive to cluster shape
4.	SOM	Distance to a cluster center Neural network where output neurons are pixels of a density map and similar cases are mapped close to each other	Good reduction of data feature dimensionality while maintaining relationships between the feature	Resulting model is a black box and creating a model is computational intensive.

VIII. CONCLUSION

The paper describes the pre and cons of the cryptanalysis, various researches by re-known researhers is being considered which will be quite help for the further understanding of the concept on cryptanalysis and also for the further research in the same field. The work presents a clear knowledge about the various techniques and researches done in the field of cryptanalysis. The study can also be further considered for the enhancement of the techniques as there is a brief description of the techniques and algorithm. The major focus of the study was over the techniques of cryptanalysis where the author have used the concept of artificial neural network in the proposed work, which actually is the future of cyptanalysis. The work presented not only summarizes the work done by the various researchers in the field of cryptanalysis but also provides supplement for the enhancement of the research work in the field of cryptanalysis.

The paper describes the pre and cons of the cryptanalysis, various researches by re-known researchers is being considered which will be quite help for the further understanding of the concept on cryptanalysis and also for the further research in the same field. The work presents a clear knowledge about the various techniques and researches done in the field of cryptanalysis. The study can also be further

considered for the enhancement of the techniques as there is a brief description of the techniques and algorithm. The major focus of the study was over the techniques of cryptanalysis where the authors have used the concept of artificial neural network in the proposed work, which actually is the future of cyptanalysis. The work presented not only summarizes the work done by the various researchers in the field of cryptanalysis but also provides supplement for the enhancement of the research work in the field of cryptanalysis.

IX. Recommendations

The presented identification techniques depend on the observation of the input-ouput of the unknown system; however a new technique could be used to identify the unknown system knowing the output of it only. This technique is known as "Blind identification", and could be a future work to develop this work.

X. AKNOWLEDGMENT

Deanship of Scientific Research of Najran University has supported this work (Project no: NU/ESCI/15/080).

XI. REFERENCE

[1] Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede. Spongent: A Lightweight Hash Function. In Bart Preneel and Tsuyoshi Takagi, editors, CHES, volume 6917 of Lecture Notes in Computer Science, pages 312–325. Springer, 2011.

[2] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanal- ysis of the full aes. In Proceedings of the 17th International Conference on The Theory and Application of Cryptology and Information Security, ASIACRYPT'11, pages 344– 371, Berlin, Heidelberg, 2011. Springer-Verlag.

[3] ShafiGoldwasser,SilvioMicali,andRonaldL.Rivest.A"paradoxical"solutiontothesig- nature problem (extended abstract). In FOCS, pages 441–448. IEEE Computer Society, 1984.

[4] Pascal JUNOD. Statistical Cryptanalysis of Block Ciphers. PhD thesis, ECOLE POLY- TECHNIQUE FEDERALE DE LAUSANNE, 2005.

[5] S. Prajapat, R. S. Thakur, "Various Approaches towards Cryptanalysis", International Journal of Computer Applications (0975 – 8887) Volume 127 – No.14, October 2015.

[6] Wolfgang Kinzel, IdoKanter, ―Neural Cryptography‖, Proceedings TH2002 Supplement, Vol. 4, 147 – 153, 2003.

[7] Einat Klein, Rachel Mislovaty, IdoKanter, Andreas Ruttor, Wolfgang Kinzel, ―Synchronization of neural networks by mutual learning and its application to cryptography‖, In proceeding of: Advances in Neural Information Processing Systems 17 ,Neural Information Processing Systems NIPS, 2004.

[8] N. Prabakaran, P. Vivekanandan, ―A New Security on Neural Cryptography with Queries‖, Int. J. of Advanced Networking and Applications, Vol. 2, Issue. 1, 437-444, 2010.

[9] R. M. Jogdand, Sahana S. Bisalapur, ―Design of an efficient neural key generation‖, International Journal of Artificial Intelligence & Applications (IJAIA), Vol.2, No.1, 60- 69, 2011.

[10] Pratap Singh, Harvir Singh, ―Cryptography in structure adaptable digital neural networks", National monthly refereed journal of research in science & technology, Vol.1, Issue.12, 35-44, 2012.

[11] DES. Data encryption standard. In In FIPS PUB 46, Federal Information Processing Standards Publication, pages 46–2, 1977.

[12] Eli Biham and Adi Shamir. Differential Cryptanalysis of the Full 16-Round DES. In Ernest F. Brickell, editor, CRYPTO, volume 740 of Lecture Notes in Computer Science, pages 487–496. Springer, 1992.

[13] Stefan Lucks. The saturation attack - a bait for two fish, 2000. preprint lucks@th.informatik.uni-mannheim.de 11214 received 14 Sep 2000.

[14] Khaled M. Alalayah, Waeil fathi, Al-Hamami H. Alaa,"Applying Neural Networks for Simplified Data Encryption Standard (SDES) Cipher System Cryptanalysis",The International Arab Journal of Information Technology (IAJIT) Vol-9 ,No-2, March 2012.

[15] Shaligram Prajapat, S. Swami, B. Singroli, R.S. Thakur, A. Sharma, D. Rajput,, "Sparse approach for realizing AVK for Symmetric Key". IRCESM 2014, Dubai UAE, IJRDET, P.P., 15-18. Google Scholar.