Classification and Identification of Classical Cipher Type Using Artificial Neural Networks

Ahmed Abd, Sufyan Al-Janabi
University of Anbar
Iraq
proahmed.j.abd@gmail.com
saljanabi@fulbrightmail.org

ABSTRACT: *In this paper, the capability of classifying the main types of classical ciphers systems is presented using Artificial Neural Networks (ANNs) starting from the simplest form of information (natural text) and ending with more complex type of classical ciphers (periodic polyalphabetic system and polygraph system with four degrees of key order). The aim of this paper is to prove that all classical ciphers can be classified or identified depending on the degree of complexity of the ciphertext. This can be done by using three levels of classification. The obtained results showed that the proposed classifier can successfully classify the classical cipher systems. This is a clear success for the proposed classifier opening further research directions and can produce informative insights on the problem of identifying and classification of ciphertext produced by modern ciphers, which is an important activity in automated cryptanalysis.*

Keywords: Artificial Neural Networks (ANNs), Classical Ciphers, Classification, Polyalphabetic System, Polygraph System

Received: 29 March 2018, Revised 4 May 2018, Accepted 16 May 2018

DOI: 10.6025/jism/2018/8/3/94-104

1. Introduction

The area of information security includes working inside the frame of cryptology which can be sub divided into cryptography (securing information from an authorized agent) and cryptanalysis (an authorized agent trying all possible solutions to obtain the original form of secure information), In cryptanalysis, if the attacker has just the ciphertext (Ciphertext-only attack), he/she should firstly determine the type of cipher to be attacked, In fact, identifying the type of ciphers can be considered as a basic functionality for any automated cryptanalysis system along with the task of identifying the language of the original cryptographic information (plaintext language). The consequent step would be finding the secret key used to hide the information in order to infer the original form of information (plaintext) [1], [2].

The classification of cipher type requires finding suitable characteristics that lead to recognizing the cipher general category and specific cipher type. The classification and identification process also include telling if the considered ciphertext does not belong to the set of ciphers being considered by the system. Given that only classical ciphers considered in the current version of this

work, it will be prudent to tell whenever the ciphertext had been produced by other ciphers that cannot be identified using the same characteristics of the classical ciphers (For example when the ciphertext was produced by some modern ciphers like DES, AES, RSA, etc.).

Classical ciphers can be classified under two general building blocks: substitution ciphers and transposition ciphers. These two classes can also be sub divided into more specific subclasses according to ability of each sub class to hide the statistics of the plaintext [2]:

• *Substitution ciphers* replaces letters in the plaintext with other letters to produce confusion (relationship between key and ciphertext is as complex as possible).

• *Transposition ciphers* rearrange letters of plaintext to produce diffusion (all plaintext letters effect all ciphertext letters).

If someone examined any text that has no replacement or rearrangement in its letters, he/she will find this text is keeping the statistics of its language. These statistics gradually hide when the degree of confusion and/or diffusion increases. This might lead the cryptanalyst who want to find a start point to attack a cryptographic system to think as the cryptographer when he/she began to increase the degree of statistics hidden along the time.

Many of artificial intelligent techniques have been used in cryptology; the most important one is the ANNs. This is mainly related to ANNs capability in estimation and identification of things. ANNs represent a simulation of human brain by converting the processes in the brain to mathematical representation and trying to solve the problems in naturally inspired pattern. This can be done by training weights that access known inputs with its outputs and giving these weights the chance to infer other cases not included in the training process [3]. ANNs include more than one way to solve problems depending on the problem itself. The reader can refer to [4] for a detailed review of the main models of ANNs. In our work, ANNs based on back propagation algorithm has been implemented using object-oriented programming to train the ciphertext classifier and test it.

Applying intelligent techniques in classical cipher cryptanalysis problems is a very typical and effective approach in order to understand the functionality of these techniques before extending them to attack more complex environment of modern ciphers such as block ciphers and public-key algorithms [5].

The remaining of this paper is organized as follows: Section 2 presents some of the related works. Section 3 shows the classifier's cipher space, while Section 4 illustrates the classifier design. Next, Section 5 presents the obtained results and discussions. Finally, Section 6 concludes the paper and outlines some directions for future work.

2. Related Work

In this section, some related earlier work is reviewed. In 2001, P. Maheshwari classified classical ciphers into four main categories (transposition, substitution, combination, and Vigenere) based on the ciphertext. He used the statistics DIU, DISU, and DISB (To be explained later) as features to recognize each group of classical ciphers. He put Vigenere ciphertext as independent part from substitution ciphers. He also identified a class of ciphers called combination ciphers which might contain other specific branches in the classification tree [6].

In 2005, J. Dunham, M-T Sun and J. Tseng presented depth cipher detection. They called ciphers encrypted with the same key as ciphers in depth. They introduced the depth attack based on finding ciphers in depth so as to break a cryptosystem without even knowing the ciphering algorithm. They firstly clustered ciphers according to their common keys. This step was called depth detection. Next, it would be possible to identify the file type of the underlying message of each cipher. Depth detection was accomplished for stream ciphers with a hit rate of 99.5 %. Indeed, ciphers in depth were further classified according to the file types of their underlying messages with an accuracy of over 90 %. The extracted features from the test samples for classification were simple ones. That could enable further performance improvement through the adoption of more complicated features [7].

In 2010, G. Sivagurunathan, V. Rajendran and T. Purusothaman classified three of substitution ciphers (Vigenere cipher, Hill cipher and Playfair cipher) using ANNs and three groups of features at which each group acts as a one cipher. They could classify the three ciphers using different texts length and different keys length in a hit rate of 100 % for Playfair cipher and 70 % - 80 % for Vigenere cipher. The ratio of classifying Hill cipher was dependent on the size of secret key [8].

In 2014, M. Nuhn and K. Knight identified and classified the set of classical ciphers mentioned by American Cipher Association (ACA) using ANNs. They achieved 58.49 % total accuracy using ANNs with more statistics and independent features. However, the weakness in this research might be the use of one classification level which produced lower classification accuracy [9].

In 2016, C. Tan and Q. Ji tried to identify some cryptographic algorithm based on ciphertext information only. They presented the used implementation architecture of the identification system. They next applied the system to identify five common block ciphers, namely AES, Blowfish, 3DES, RC5 and DES. Based on the experimental results, they concluded that identification rate can obtain around 90% if keys are the same for training and testing ciphertexts. When they used different keys for training and testing ciphertexts, identification system can still identify AES from the other cryptographic algorithms with a high identification rate in one to one identification [10].

3. Classifier's Cipher Space

In this work, the proposed ANN classifier has four main tasks:

1. The first task is to determine if any text is encrypted or not.

2. The second task (if the text is encrypted) is to determine the classical cipher general group (classification).

3. The third one is to specify the specific ciphers from its general group with a mark that recognize its type (identification).

4. Finally, the fourth task is to tell if the ciphertext does not belong to the considered classical ciphers, i.e. when it had been generated by other cipher types that have degree of confusion and/or diffusion higher than classical ciphers.

The starting point for these four tasks can be the natural text or plaintext itself (text without any encryption process). This text has zero security because it keeps all the statistics of its language. So, by simple classification criteria, natural text can be recognized from any encrypted text. After ensuring that the text is encrypted using some encryption technique, it would be possible to put the encrypted text (ciphertext) under one of the following three general categories of classical ciphers: Transposition system, substitution system, combination system (combined substitution and transposition system).

The classifier treats all transposition techniques as the same so there is no classification of transposition ciphers in this work except for the general category. Indeed, the classifier treats combination system as a combination between simple substitution cipher (explained later) and any type of transposition cipher.

When the classifier classifies any text under one of the three general categories that are mentioned above, *Level1* is must be finished before the starting of *Level2,* which begins with classification of substitution system into sub classes. The substitution system is divided in this work into three classes:

1. *Monoalphabetic substitution system:* This class includes any cipher that go to increase confusion property by using one-to-one mapping between plaintext and ciphertext like Caesar cipher, Affine cipher, Atbash cipher and simple substitution cipher.

2. *Periodic polyalphabetic substitution system* (Vigenere cipher): This class uses one-to-many mapping between plaintext and ciphertext by repeating secret key along plaintext to increase confusion property more than Monoalphabetic substitution system.

3. *Polygraph substitution system*: This includes any cipher that increases confusion property by encrypting more than one letter at a time. So, this type of system can be considered to work much like a block cipher. In this work, three of polygraph ciphers are considered: Playfair cipher, Hill3 cipher (with 3*3 key matrix), and Hill4 cipher (with 4*4 key matrix).

The classifier treats all Monoalphabetic substitution ciphers as the same, so there is no classification of Monoalphabetic substitution ciphers accept as a general class. Also, the classifier can only identify periodic polyalphabetic substitution and considers non-periodic polyalphabetic substitution system to be outside the classification level.

If the classifier classified the encrypted text as a polygraph substitution system then *Level 2* is finished and *Level 3* will start to see if the encrypted text had been encrypted by one of the three polygraph ciphers mentioned above or it is out of the considered classical cipher space.

The classifier depends in its function on some of statistics or measures that can be extracted from the text. Hence, the classifier ignores many of ciphers types that can be recognized just by looking at the encrypted text like Baconian cipher.

It is important to notice that some of classical ciphers have relatively high level of complexity when an attacker tries to break or cryptanalyze them, but it is easy to recognize them from ciphertext. On the other hand, some other ciphers like Caesar cipher can be broken by simple brute force attack but the identification of its type is more difficult process. This gives us an additional insight on the necessity of ciphertext classification.

There are two types of characteristics (features), the first one is a group of features owned by single cipher and no more cipher have these features, and the second type is a group of features shared by a group of ciphers and each cipher has a degree of each feature like features used in this paper.

The most important statistics that have been used in this work are explained in Table 1. These statistics represent the features or characteristics that can be extracted according to available resources. These statistics in general are the most obvious measures that can lead to classify classical ciphers using artificial intelligence. They have been used in the field of cryptology in two directions, the first one is to increase the security of cryptographic system and the second is to find the weakness in the system according to capability that the attacker have [11], [12]. In this work, the attacker is assumed to only have the ciphertext.

4. The Classifier Design

Classification process is accomplished in three levels. For each level, almost the same sequence steps are considered. These steps begin from preprocessing that includes reading of a big group of plaintexts and encrypting them by using the classical ciphers that are intended for classifying. Then from these encrypted texts (Ciphertexts) we can extract features that lead to recognize cipher type, the extracted features are used as inputs to the ANN.

The total number of weights in the *ANN* is determined using the following equation:

$$W = (In * H) + H + (H * Out) + Out \quad (1)$$

where *W* represents the total number of weights, *In* represents the number of inputs nodes, *H* represents the number of hidden nodes, and *Out* is the number of outputs nodes.

The weights are generated randomly then it will be adjusted in the training process. The output of each ANN hidden node (*h*) is calculated using the hypertan activation function, while sigmoid activation function is used to calculate the output of each ANN outputs node (*out*). The following two equations are used for the activation function respectively:

$$H = tanh\ (h) \quad (2)$$

$$Out = 1/(1+exp(-out)) \quad (3)$$

The ANN algorithm consists of two phases, the first phase is used to obtain the actual output of the classifier (feed forward), while the second phase is used to update the weights by obtaining the difference between the desired output (dataset) and the actual output (classifier output), this phase is called back-propagation. The following steps represent the proposed ANN algorithm that will be executed for each classification level:

- **Step 1:** Let *X* be the input nodes, Let *WXH* be the weights between the input layer and the hidden layer, Let WHO be the weights between the hidden layer and the output layer. Let HB be the bias on hidden layer *j*. Let OB be the bias on output k. Initialize weight vectors (set them to small random values [-0.5, 0.5]. Initialize learning rate (α) ($0 < \alpha \leq 1$).
- **Step 2:** count = 0
- **Step 3:** For each training row do steps 4-10
- **Step 4:** For each hidden unit, ($H_j, j = 1,.., n$), find:

Statistics	Statistics	Description
1	DIU	The difference in frequency distribution ratio of single English letters in alphabetical order (A…..Z).
2	DISU	The difference in frequency distribution ratio of single English letters in descending order (E, A, T…..).
3	DISB	The difference in frequency distribution ratio of double English letters in descending order (more frequent sections have the greater ratio). Ciphertext with four letters have three sections.
4	Bigrams (BIG)	The difference in frequency distribution ratio of double English letters in descending order (more frequent section have the greater ratio) without intersection between each two sections (Ciphertext with four letters have just two sections).
5	Trigrams (TRI)	The difference in frequency distribution ratio of tribal English letters in descending order (more frequent section have the greater ratio) without intersection between each two sections (Ciphertext with six letters have just two sections).
6	Quadgrams (QUA)	The difference in frequency distribution ratio of quadruple English letters in descending order (more frequent section have the greater ratio) without intersection between each two sections (Ciphertext with eight letters have just two section).
7	Caesar (CAE)	Show if can be treat the attended text as a group of Caesar texts or not.

Table 1. Statistical measures used in the classification of classical ciphers

$$h_j = HB_j + \sum_{i=1}^{n} X_i WXH_{ij} \tag{4}$$

$$H_j = f(h_j) \tag{5}$$

where f(.) is a hypertan activation function.

• **Step 5:** For each output unit, (O_k, $k = 1,.., m$), find:

$$o_k = OB_k + \sum_{j=1}^{m} h_i WHO_{jk} \tag{6}$$

$$O_k = f(o_k) \tag{7}$$

where f(.) is a sigmoid activation function.

• **Step 6:** For each output unit (O_k, $k = 1,.., m$), receive a target pattern corresponding to the input training pattern then:

- Compute the error information term using the following equation:

$$\delta_k = (d_k - O_k) f'(o_k) \tag{8}$$

where d is the desired output.

- Calculate its weight correction term (used to update WHO_{jk} later) using the following equation:

$$\Delta WHO_{jk} = \alpha \delta_k H_j \quad (9)$$

- Calculate its bias correction term (used to update w_{0k} later):

$$\Delta OB_k = \alpha \delta_k \quad (10)$$

• **Step 7:** For each hidden unit ($H_j, j = 1,\ldots, h$):

- Sum its Delta inputs using the following equation:

$$\delta_{ej} = \sum_{k=1}^{h} \delta_k WHO_{jk} \quad (11)$$

- Multiply by the derivative of its activation function to calculate its error information term using the following equation:

$$\delta_j = \delta_{ej} f'(h_j) \quad (12)$$

- Calculate its weight correction term (used to update WXH_{ij} later) using the following equation:

$$\Delta WXH_{ij} = \alpha \delta_j X_i \quad (13)$$

- Calculate bias correction term (used to update HBk later) using the following equation:

$$\Delta HB_j = \alpha \delta_j \quad (14)$$

• **Step 8:** For each output unit (O_k, $k = 1,.., m$) update its bias and weights ($j = 0,\ldots, h$) using the following equation:

$$WHO_{jk}^{t+1} = WHO^t_{jk} + \Delta WHO^t_{jk} \quad (15)$$

• **Step 9:** For each hidden unit ($H_j, j = 1,..., h$) update its bias and weights ($i = 0,\ldots, n$) using the following equation:

$$HB_{ij}^{t+1} = HB_{ij}^t + \Delta HB_{ij}^t \quad (16)$$

• **Step 10:** count = count+1

• **Step 11:** If count < maxepoch, then go to Step 4.

In Level 1, the classifier is trained to classify ciphers under the main categories using the statistics (DIU, DISU and DISB). In Level 2, the classifier is trained to classify substitution ciphers and identify them by using the five statistics (DISU, BIG, TRI, QUA and CAE). Finally, in Level 3, the classifier is trained to classify and identify polygraph substitution ciphers by using the three statistics (B, T and Q), as shown in figures 1, 2, and 3, respectively.

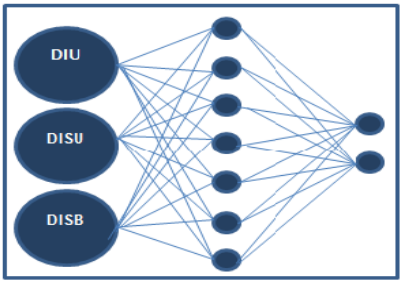


Figure 1. Architecture of classifier's Level 1

Figure 4 shows the classification diagram of the three levels and the desired output of each class to be identified. The dataset used to train the classifier constitutes from more than million letters encrypted by the ciphers mentioned above and other ciphers that create the boundaries of the classification area like Auto key cipher and Hill cipher with 5*5 key matrix. In encryption process, random keys are used with every encrypted text to coverage greater area for training and testing processes giving 80% from the dataset for training process and 20% for testing process. The numbers and symbols ignored and just the letters considered without spaces, so every text can be examined after isolating the letters from the numbers and symbols.

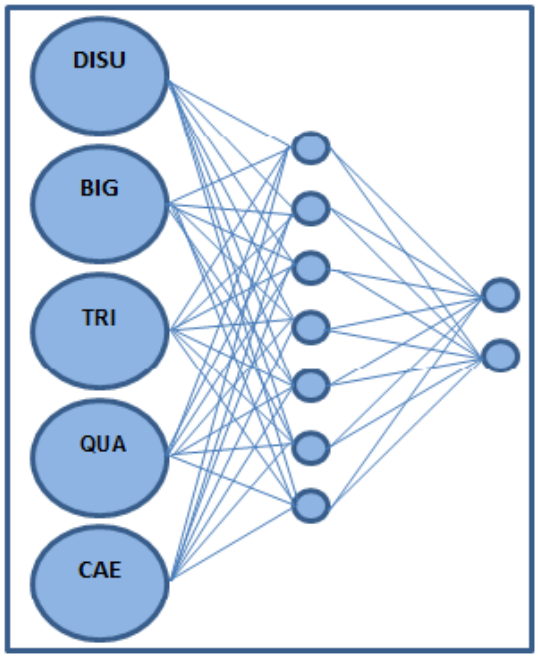


Figure 2. Architecture of classifier's Level 2

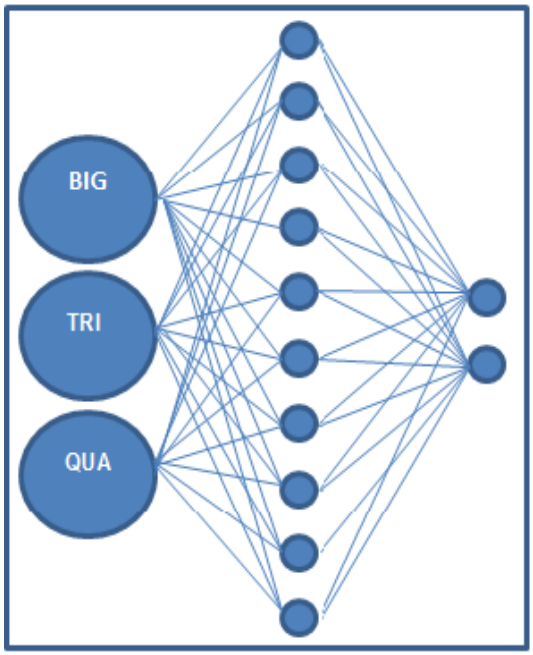


Figure 3. Architecture of classifier's Level 3

The proposed system for classification and identification of classical cipher has been implemented using back propagation algorithm with one hidden layer for each level. Table 2 shows the parameters that are used in the proposed ANN.

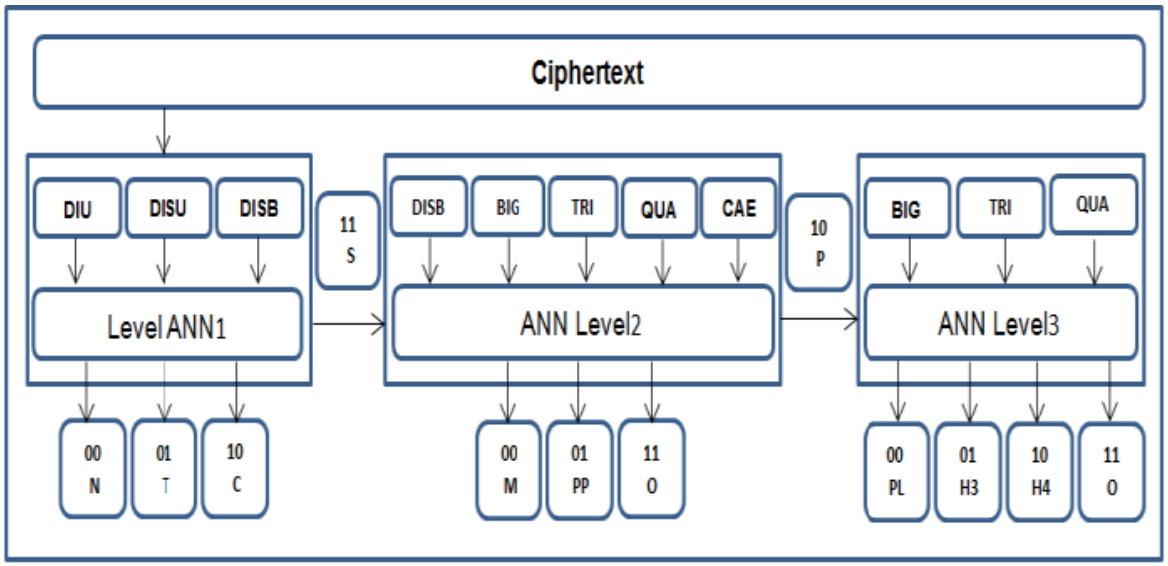


Figure 4. Classification diagram

	Inputs	Hidden nodes	Outputs	Epochs	Learning rate	Momentum
Level 1	3	7	2	500	0.01	0.01
Level 2	5	7	2	500	0.01	0.01
Level 3	3	10	2	100	0.1	0.1

Table 2. Parameters of ANN used in the Classification Process

5. Results and Discussion

The proposed ANN classifier has been executed for each level using appropriate statistic measures and suitable number of examples (Dataset). The obtained results for training and testing processes are shown in Table 3.

Concerning the testing phase of the classification system, the results have shown that 99.6% of testing samples can be classified correctly, as shown in Table 4. All texts have been examined with same length and different keys. The obtained results clearly indicate a success for the proposed classifier. This is due to the ANNs capability in classification issue and the division of

Levels	Result (samples)	Dataset (kb)
Level 1	100 %	11724
Level 2	100 %	8793
Level 3	100 %	8793

Table 3. Results of Training and Testing Processes

classification process to three levels which help ANN to determine the separated line between each two classes with high score. To see how the statistics measure is differentiated among the classes, figures 5, 6, and 7 show the curves of each class.

Cipher Type	Texts Number	Correct Texts
Nutural text	50	50
Transposition	50	50
Caesar	50	50
Simple substitution	50	50
Combination	50	50
Vigenere	50	50
Playfair	50	48
Hill3	50	50
Hill4	50	50
Hill5	50	50
Auto key	50	50

Table 4. Testing of the Classification System

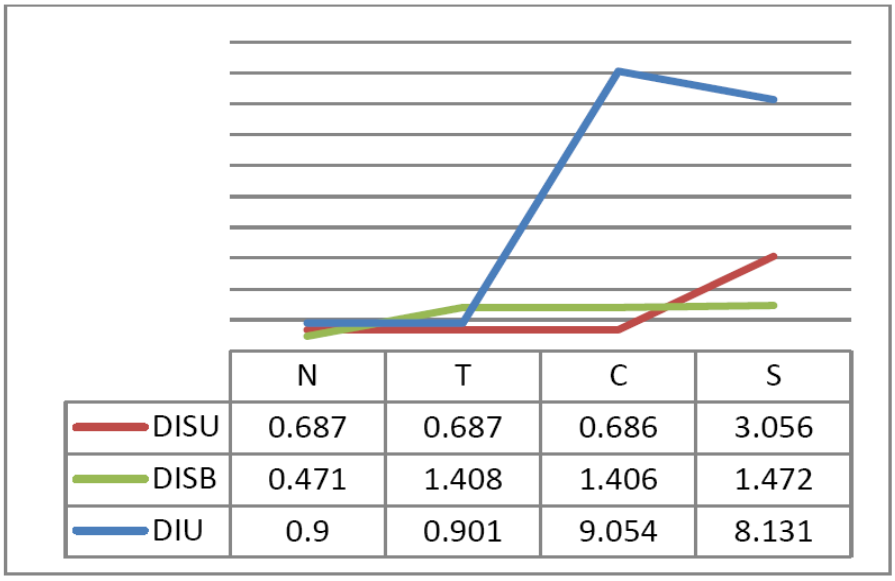
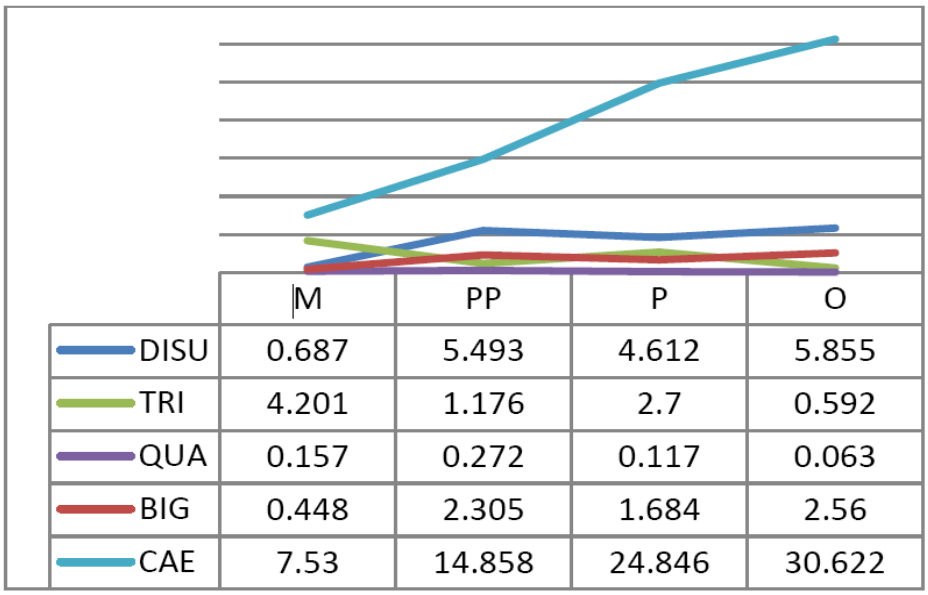


Figure 5. Relationship between texts and its features in Level 1

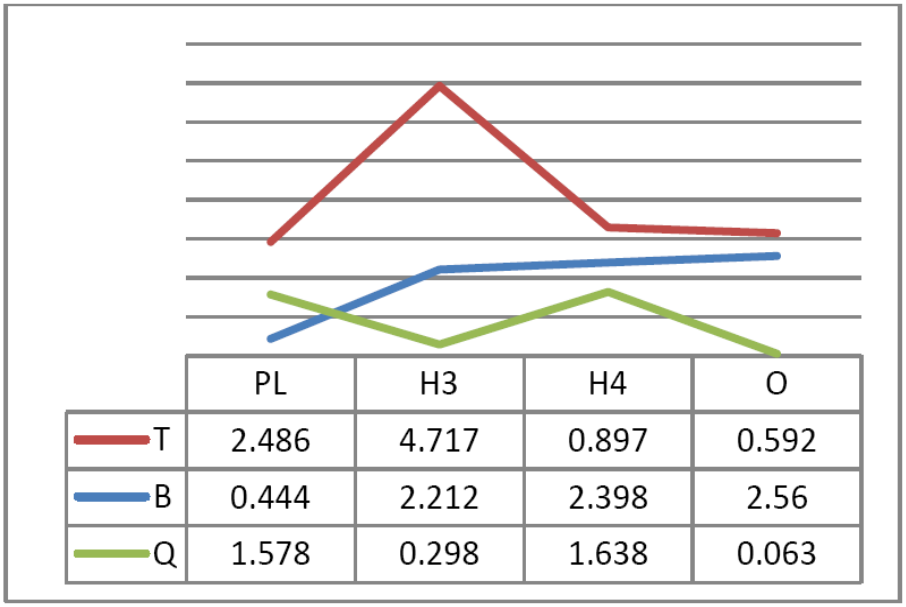
From the resulted curves, we can see how the proposed classifier can draw wide separated line between each category and around all categories wants to classify. The width of the separated line considered as the measurement of the success for ANNs in classification process, such that, if the separated line is very narrow and there are intersections in different areas between each category, in this case, we can say that ANNs cannot implement classification process correctly.

In other side, if the separated line is very wide, in this case the classification process can be implemented using just nested if statement rules. Usually the success of ANNs in classification process mainly depends on the previous knowledge in ANNs capabilities and theoretical implementation of classification system. This leads us to seek about standard ANN's parameters for each problem which is considered as challenge nowadays. So, the selection of ANN's parameters is done by experimental choice, specifically when we talking about the number of hidden layers and nodes or learning rate value.



	M	PP	P	O
DISU	0.687	5.493	4.612	5.855
TRI	4.201	1.176	2.7	0.592
QUA	0.157	0.272	0.117	0.063
BIG	0.448	2.305	1.684	2.56
CAE	7.53	14.858	24.846	30.622

Figure 6. Relationship between texts and its features in Level 2



	PL	H3	H4	O
T	2.486	4.717	0.897	0.592
B	0.444	2.212	2.398	2.56
Q	1.578	0.298	1.638	0.063

Figure 7. Relationship between texts and its features in Level 3

Acknowledgment

Authors would like to sincerely thank Dr. Belal Al-Khateeb for his helpful insights, discussions, and comments on this work.

6. Conclusion

In this work, automated cryptanalysis of classical ciphers has been considered. A basic step for achieving this is the process of classification and identification of ciphertext. A back propagation ANN has been for this purpose. The classification process can be done by measuring the degree of confusion and diffusion inferred from the two main building blocks of most cryptographic

systems. Automated attack has shown to be an effective way to destroy a cryptographic system or to find its weaknesses. It can be seen that there is a divide line between classical systems and modern systems. This can be used in two directions; the first one is in the isolation of classical ciphers by considering this line as an upper boundary, and the second by considering this line as a start point to classify or identify modern ciphers. The issue of classification and identification of modern ciphers might be considered in a subsequent paper. Also, using intelligent techniques for finding the secret key of the identified ciphers can be considered as another future work direction.

References

[1] Haizel, K. N. (1996). Development of an automated cryptanalysis emulator (ACE) for classical cryptogram, M.Sc. Thesis, Faculty of Computer Science, University of New Brunswick, New Brunswick.

[2] Stallings, W. (2014). Cryptography and Network Security Principles and Practices, 6th ed., Upper Saddle: Pearson Education, Inc.

[3] Kriesel, D. (2017). "A brief introduction to neural networks, 2005. Available at: http://www.dkriesel.com/en/science/neural_networks [Accessed on 12/11/2017].

[4] Tino, P., Benuskova, L, Sperduti, A. (2015). Artificial neural network models, Appeared in Springer Handbook of Computational Intelligence, J. Kacprzyk and W. Pedrycz (Eds.), Part D, 455-471, Springer..

[5] Prajapat, S., Thakur, R. S. (2015). Various approaches towards cryptanalysis, *International Journal of Computer Applications*, 127 (14), 15-24, October.

[6] Maheshwari, P. (2001). "Classification of Ciphers, Master of Technology Thesis, Department of Computer Science and Engineering, *Indian Institute of Technology*, Kanpur.

[7] Dunham, J. G., Sun, M., Tseng, C. R. (2005). Classifying file type of stream ciphers in depth using neural networks, The 3rd ACS/*IEEE International Conference on Computer Systems and Applications*, Cairo, Egypt, 6 January.

[8] Sivagurunathan, G., Rajendran, V., Purusothaman, T. (2010). Classification of substitution ciphers using neural networks, *International Journal of Computer Science and Network Security*, 10 (3), 274-279, March.

[9] Nuhn., Knight, K. (2016). "Cipher type detection, Information Sciences Institute, University of Southern California, EMNLP, 2014. Available at: https://www.semanticscholar.org/paper/Cipher-Type-Detection-Nuhn-Knight. [Accessed on 10 June 2016].

[10] Tan, C., Ji, Q. (2016). "An approach to identifying cryptographic algorithm from ciphertext, *The 8th IEEE International Conference on Communication Software and Networks*, 19-23.

[11] Bahaa Eldin, A. M. (2004). Intelligent Systems for Information Security, Ph.D. Thesis, *Computers & Systems Engineering* Ain Shams University, Egypt.

[12] Carter, B., Magoc, T. (2017). Introduction to classical ciphers and cryptanalysis, A Technical Report, 11 Sep. 2007. Available at: http://www.citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.125.8165. [Accessed on 5 February 2017].