JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

# Affine Neural Network Cryptography

**Vikas Thada[1], Utpal Shrivastava[2]**

[1] Amity Institute of computer science and Engineering,Amity University, Haryana, India
[2] Amity Institute of computer science and Engineering,Amity University, Haryana, India

**Corresponding Author: vthada@ggn.amity.edu, Tel.: 9958324522*

**Available online at: www.ijcseonline.org**

18/May/2018, Published: 31/May/2018

***Abstract*—** In the recent years the main concern in computers and internet has been information security. Researchers and developers are mainly concerned with services which provides secure exchange of information over the internet and networks. The focus has been on 3 security triads: Confidentiality, Integrity, and Availability. The one simple way of achieving security is by the use of cryptography. There are number of features a chaotic systems possess and can be utilized within cryptography. Features like sensitivity to initial conditions/system parameters,ergodicity, mixing properties, deterministic dynamics, and structure complexity. Cryptosystems which are chaos based as compare to conventional provide high levels of security and yields betterresults [2].In this paper a hybrid approach using the concept of affine cipher and chaotic neural network (CNN) is proposed. Data is first encrypted using affine cipher and result of this is fed to the CNN. The reverse operation is performed for decryption. The experiment was carried out in MATLAB 2012a. Secrecy of the proposed work comes from the fact that total four keys need to be kept secret: two from affine and two from CNN. Further the chaos as part of CNN also add to the security.

***Keywords*—** affine, encryption, decryption, chaotic, neural, network

## I. INTRODUCTION

Now a day's data security has become an important aspect in every type of communication. The ultimate surety of data demands that it is to be known only to the sender and recipient and this forms the principle of confidentiality in the realm of cryptography. In today's world because of proliferation of networks be it wired or wireless sharing of information has become so easy and fast. Thanks to the concept of pervasive and mobile computing. This entails us to provide certain measures for the confidentiality of sensitive and private information before it leaves from source and reaches to destination and the fundamental concept we use is cryptography. Cryptography is the art of securing data by encoding it in an unreadable form. For achieving cryptography two varied techniques can be utilized: Symmetric & asymmetric. Symmetric encryptions make use of single key for enciphering and deciphering the data whereas asymmetric make use of two different keys: public and private. Conventional cryptographic techniques and algorithms such as DES, AES, Blowfish, IDEA, RC4, RSA etc. are very much mathematical in nature and based on number theory. Some of the algorithms require high processing power specially based on asymmetric key cryptography and very time consuming and not suitable for image and video encryption. Chaos is one of the realm that seems perfect for cryptography be it data/image/video and amalgamation of conventional and chaos based will definitively make system more secure

## II. RELATED WORK

Aihara et.al [1] was the pioneer in the field of chaotic neural networks for cryptography. It was Aihara[1] who clearly demonstrated neural network based on chaotic sequences consisting of chaotic neurons. Chaotic neural network(CNN) was a special neural network exhibiting chaotic dynamic behavior. Since then a researcher have delved into this topic for text/image/video. P.Singla et al.[2] and S.Lokesh et al[3] designed a pseudo-random binary sequence generator based on CNN. The CNN based generator of [2] was for cryptographic applications and made use of chaos features whereas [3] used cubic map and the piece-wise linear chaotic map just because chaotic map exhibits high sensitivity and randomness property. Results of both [2,3] were promising and opened new directions in the area of pseudorandom sequence generator. N.Abdoun[4] presented a new CNN based hash function and compared it to existing Hash functions. He showed some of the statistical attacks (Uniformity and NIST) were easily launched against simplechaotic maps. H.kaur et al [5] proposed a method of CNN based for enciphering and deciphering the data. It was concluded that proposed CNN based cryptography scheme is sensitive to some system parameters, initial conditions, and topological transitivity. J.Singh [12] also used CNN along with caeser cipher for encryption and decryption of plain text data. M.Chauhan[13] experimented with ANN based, CNN based and chaotic based Network and compared the results of image encryption using AES algorithm using PSNR and MSE. N.K.Kamila[6] combined the concepts of LSB steganography and CNN based cryptography for the encryption and decryption digital image. The combined approach provide high security and message/image is resistive to attacks. Experimental analysis proved robustness of the proposed technique. K.Qin et al.[7] discussed the issues related to security and efficiency of a CNN based cryptographic algorithm.Qin et al [7] used a cryptographic algorithm based on the Delayed CNN. W.Yu et al.[8] proposed a chaotic Hopfield neural networks based enciphering scheme with time varying delay. The proposed CNN generated binary sequences and used for masking plain text.. Simulation results proved the feasibility and effectiveness of the proposed work. I.Dalkiranet al.[9] discussed that some properties of chaotic systems such as synchronization, fewness of parameters were not good for cryptology and to overcome the preceding problems of CNN the with the help of Artificial Neural Network (ANN)., dynamics of Chua's circuit namely x, y and z were modeled.Dalkiran[9] used a feed-forward Multi-Layer Perceptron (MLP) and trained it with Bayesian Regulation back propagation algorithm. Experimental results showed that this was the suitable network structure. Similar kind of work was carried byA.S.Mhetras et al.[14]. Their ANN was trained by trying different structures and learning algorithms. The difference was that [9] used Bayesian regulation back propagation algorithm whereas [14] used Levenberg-Marquardt back propagation algorithm. N. Crook et al.[10] speculated that for controlling linear and non-linear systems chaotic dynamics are significantly easier. The reason behind that they require tiny timed perturbations to constrain them within specific Unstable Periodic Orbits (UPOs). N.Crook[10] explored possibility that in response to specific dynamic input signals a network can self-select UPOs. H.Zhenya et al. [11] has used the concept of CNN based coupled map network in the field of information processing. They proposed one-dimensional, two-way coupled map network and as per the proposed network they modified the definition of an auto-associative matrix. Experimental analysis have resulted in improved associative success rate and recall speed over existing methods. A.Jain et al.[15] investigated the strength and security of chaotic image encryption algorithm based on logistic map and uses three keys. They showed that algorithm is vulnerable to known-plaintext/ciphretext. They also reported that algorithm is affected by some parameters namely low key space and insensitivity with respect to change of plain-image. Experimental and theoretical analysis suggest that scheme is not suitable for applications involving high security.

## III. CHAOS THEORY

Exact definition of the chaos is not known but as given by [6] which says that chaos in something in which futures is determined by present but a little approximation in present will not approximately determine future. As per [Conference] chaos has been observed in nature: dynamics of satellites, fluid dynamics, mechanical systems, magnetic field of celestial bodies and many other. Application of chaos includes communication and signal processing, cryptography (this paper is covering), digital image encoding, sound engineering, chaotic transport. Chaotic theory has been researched and implemented in the field of cryptography for its noise like behavior. Crucial to the chaos theory is the concept of nonlinear dynamical system whose behavior is dependent on initial conditions. By changing different initial values to chaos based system random signals can be generated and these sequences are known as chaotic sequences. The commonly employed and highly studied method for one-dimensional system capable of generating chaotic sequence is logistic map:

$$X_{n+1}=r\ X_n\ (1-X_n)$$

r is control parameter and it controls the behavior of the logistic map. Initial value of r and X0 must be provided.

Chaotic systems are sensitive to system parameters, initial conditions, and aperiodic dynamics. Because of these properties chaotic systems are a good choice for cryptography. [X] observed various equivalence between fundamental properties of chaotic systems and cryptographic system. Ergodicity is equivalent to confusion, Mixing property, sensitivity to initial conditions and mixing property is equivalent to diffusion, deterministic dynamics is equivalent to deterministic pseudo randomness.

## IV. AFFINE CIPHER

Affine cipher is an encryption scheme or type of substitution cipher, in which each English alphabet is represented by its numeric values starting from 0 for A, 2 for B upto 25 for Z. Then using an encryption method which is nothing but a mathematical formula (discussed shortly) every alphabet is converted to some other alphabet. During the decryption process reverse formula is applied and original text is recovered from encrypted text.

The encryption scheme is written in the following form:

$$\boldsymbol{E(x) = (px + r) mod\ 26}$$

Here E(x) is the affine encryption function where x is the integer value of English alphabet as discussed earlier to this function and p and r are (appropriately chosen) integers that work as constants and serve as key for this affine cipher. Changing different values of p and r results in different versions of the affine scheme. Taking mod by 26 is to confining the numerical value E(x) within 0 and 25.

### 4.1 Encryption Using Affine Cipher

The affine cipher is a type of substitution cipher in the category of mono alphabetic cipher where each letter encrypts to one other letter, and back again following the rules of standard substitution cipher.

Considering the numerical values for the alphabets as given below:

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Following the mathematical formula as shown above first the letters of an alphabet of size M (26 in this case) are converted to their numerical equivalent integers. After these using concepts of modular arithmetic same alphabet is transformed into an integer that is the corresponding cipher text for the plain text under consideration. The encryption formula for each alphabet is

$$\boldsymbol{E(x) \quad = \quad (px + r) \; mod \; M}$$

Where M is total number of possible alphabets in the set (26 in English) , known as the size of the alphabet and p and r are the key of the affine cipher. The value p must be chosen such that p and M arecoprime i.e. GCD (a, M) =1.

### 4.2 Decryption Using Affine Cipher

If we take y = E(x) = (px + r) mod 26, then we can solve the formula in terms of y for the value of x and can easily find out E−1(y) known as inverse that is, if y = (px + r) (mod 26), then y − r = px (mod 26)

By dividing both sides by mod 26 we get

$$\boldsymbol{px \quad = \quad (y - r) \; mod \; 26}$$

Multiplying both sides by $p^{-1}$ mod 26 we get then

$$\boldsymbol{x \quad = \quad p^{-1}(y - r) \; mod \; 26}$$

So the formula for affine decryption becomes

$$\boldsymbol{E^{-1}(y) \quad = \quad p^{-1}(y - r) \; mod \; 26}$$

Where $p^{-1}$ is known as MMI (modular multiplicative inverse) of a modulo M. I. The MMI satisfies the following equation

$$\boldsymbol{1 \quad = \quad p.p^{-1} \; mod \; M}$$

The MMI of a number pcan only exists when GCD (p, M) = 1. This is the requirement for the affine decryption.

### 4.3 Algorithm of Euclid

For finding greatest common divisor (GCD) or highest common factor(hcf) algorithm of Euclid is used. The algorithm is based on the following two observations:

If y|x then GCD (x, y) = y.

Where y|x means y divides x. The basis of Euclid's algorithm is division theorem.

If x = yt + r, for integers t and r, then GCD(x, y) = GCD(y, r). Here t is quotient and r is remainder.

Indeed, every common divisor of x and y also divides r. Thus GCD(x, y) divides r.

### 4.4 The Extended Euclidean Algorithm

The basis of Extended Euclidean algorithm is Euclid Algorithm. The algorithm is extended form of Euclid algorithm to find two values x and y such that

d=gcd(a,b)=ax+by (1)

From the equation (1) two more equations can be written provided d=gcd(a,b)=1

ax≡d mod b => ax≡1 mod b => x≡ $a^{-1}$mod b (2)

by≡d mod a => by≡1 mod a => y≡ $b^{-1}$mod a (3)

where x and y are known as modular multiplicative inverse of *a mod b* and *b mod a* respectively.

The algorithm is given below:

```
EXTENDED_EUCLID(a,b)

1 if b == 0

2     return (a,1,0)

3 else  (d1, x1,y1)=EXTENDED_EUCLID(b,a mod b)

4     (d,x,y)=(d1,y1,x1- (a/b)*y1)

5 return (d,x,y)

Note: (a/b) in line no 4 is integer division
```

The algorithm make use of Euclid algorithm in line number 3 and then using back substitution finds the value of x and y. The example will simply increase the length of the paper so reader is advised to search net for an illustrative example.

## V. CHAOTIC NEURAL NETWORK ENCRYPTION

Chaotic neural network is a special type of artificial neural network where the weights to neuron and biases are completely determined by a chaotic sequence. In order to apply CNN for encryption and decryption purpose the research work assumes input as an array of bytes and L is the number of such bytes, then encryption using logistic map proceeds as:

```
1. Input plain text INP and convert into numeric value(0-255)
2. Input initial parameters r and X(0) for logistic map.
3. Store length of input into L.
4. Generate chaotic sequence using the equation : $X_{n+1}$=r $X_n$ (1-$X_n$) where n=0,1,…L-1
5. Normalize the generated sequence X(0),X(1)….X(L-1) considering range of byte is 0-255.
6. Convert normalized chaotic sequence into binary and store in a matrix B of size Lx8.
7. For i=1 to L
    a. FOR j=1 to 8
        i. FOR k=1 to 8
            1. If Bij==0 and j==k then Wjk=1
            2. Elseif Bij==1 and j==k then Wjk= -1
            3. Elseif j<>k then Wjk=0
        ii. End For
    b. If Bij==0  then$\theta_i$ = -0.5 else $\theta_i$ = 0.5
    c. End For
    d. INP1$_i$=F($\sum_0^7 Wi * INPi + \theta i$)
    e. Convert INP1$_i$ back to decimal and store at ith position
8. End For
9. Display cipher text by converting numeric INP1 to character.
```

The decryption algorithm is exactly same with the difference the cipher text produced by encryption algorithm becomes input to the decryption algorithm. One important point to note here is that input text to the CNN in encryption is the output of the affine cipher. Similarly, in decryption algorithm output of CNN becomes input to the affine cipher whose output gives us plain text back.

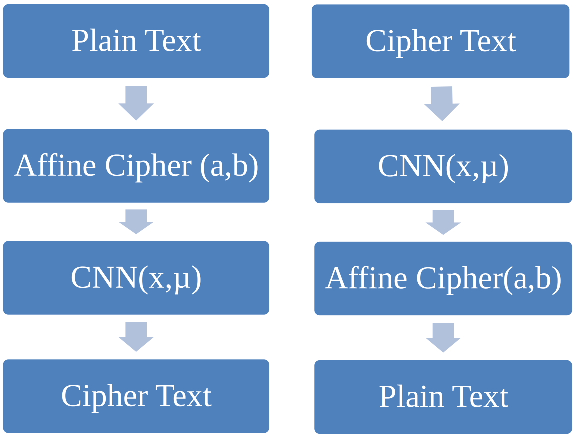

**Figure 1: Proposed hybrid encryption/decryption scheme**

## VI. EXPERIMENTS AND RESULTS

The functions were written for Euclid, extended Euclid, affine cipher encryption, decryption, CNN encryption and decryption in octave 4.2.0 on windows platform. Experiment was carried out with different possible values of keys (a,b) for affine cipher and (x,mu) for CNN. Some of the results with different text inputs are shown below in tables 1-3.

**Table 1: Affine CNN cryptosystem example 1**

| Encryption Input Text:'2+2 is 4' | | |
|---|---|---|
| Numeric Conversion | AffineE(5,7) | CNNE(0.75,3.9) |
| 50 43 50 32 105 115 32 52 | 0 222 0 167 18 68 167 10 | 156 73 160 41 189 40 116 10 |
| Decryption Input Text: 156 73 160 41 189 40 116 10 | | |

| CNND(0.75,3.9) | AffineD(5,7) | Output |
|---|---|---|
| 0 222 0 167 18 68 167 10 | 50 43 50 32 105 115 32 52 | ’2+2 is 4’ |

**Table 2: Affine CNN cryptosystem example 2**

| Encryption Input Text:’cnn& affine’ | | |
|---|---|---|
| Numeric Conversion | AffineE(3,2) | CNNE(0.75,3.9) |
| 99 110 110 32 38 32 97 102 102 105 110 101 | 42 75 75 98 116 98 36 51 51 60 75 48 | 140 234 224 251 205 21 248 62 92 220 75 124 |
| Decryption Input Text: 140 234 224 251 205 21 248 62 92 220 75 124 | | |
| CNND(0.65,2.9) | AffineD(5,7) | Output |
| 42 75 75 98 116 98 36 51 51 60 75 48 | 99 110 110 32 38 32 97 102 102 105 110 101 | ’cnn& affine’ |

**Table 3: Affine CNN cryptosystem example 3**

| Encryption Input Text:'Hell $%@#!' | | |
|---|---|---|
| Numeric Conversion | AffineE(3,17) | CNNE(0.65,2.9) |
| 72 101 108 108 32 36 37 64 35 33 | 233 63 84 84 113 125 128 209 122 116 | 233 59 84 87 112 126 129 210 123 119 |
| Decryption Input Text: 233 59 84 87 112 126 129 210 123 119 | | |
| CNND(0.65,2.9) | AffineD(3,17) | Output |
| 233 63 84 84 113 125 128 209 122 116 | 72 101 108 108 32 36 37 64 35 33 | 'Hell $%@#!' |

Correlation is a kind of relationship between two variables. It is denoted by a value between -1 and 1. Positive 1 is for positive correlation and -1 is for negative correlation. In the case of cryptography negative correlation indicates no relationship as such exist between plain text and cipher text. In other words cipher text does not give any clue as what is the corresponding plain text. Correlation of input plain text and output cipher text was calculated for some fixed values of (a,b) and variable values of x and muSome of the results are shown below:

**Table 4: Correlation between plain text and cipher text for different x and mu values**

| Input Text:”affinecipher” | | | | | |
|---|---|---|---|---|---|
| | Corr(PT,CT) ,mu=0.9 | Corr(PT,CT) ,mu=1.9 | Corr(PT,CT) ,mu=2.9 | Corr(PT,CT) ,mu=3.9 | Corr(PT,CT) ,mu=4.9 |
| x=0.10 | -0.48 | 0.54 | 0.32 | 0.08 | 0.34 |
| x=0.20 | -0.52 | 0.27 | 0.10 | 0.26 | 0.34 |
| x=0.30 | -0.42 | -0.50 | -0.26 | 0.43 | 0.34 |
| x=0.40 | -0.40 | -0.73 | -0.65 | 0.14 | 0.34 |
| x=0.50 | -0.43 | -0.54 | -0.82 | 0.01 | 0.34 |
| x=0.60 | -0.39 | -0.54 | -0.62 | 0.12 | 0.34 |
| x=0.70 | -0.37 | -0.52 | -0.56 | 0.26 | 0.34 |
| x=0.80 | -0.37 | -0.65 | -0.46 | 0.02 | 0.34 |
| x=0.90 | -0.32 | 0.01 | -0.21 | 0.24 | 0.34 |

The correlation between original plain text and cipher text obtained after CNN encryption turns out to be a good value (negative and < 0) for different values of mu=0.9,1.9,2.9 ,3.9 and x ranging from 0.10 to 0.9 with step size of 0.10. But for the values of mu=4.9 to 9.9 step size 1.0 the correlation between plain text and input cipher text is same. This indicates that values of my does not affect the encryption process and same cipher text is obtained for all values of mu from 4.9 to 9.9.

The results indicate that combining hybrid approach of affine cipher and chaotic neural network for text encryption including special symbols, digits is strong encryption technique. Further an attacker needs to grab 4 keys to successfully decrypt the plain text. Two keys (a,b) are required for affine transformation and two keys (x, mu) required for CNN. The experiment tried a slight change is x and mu of 0.1 during decryption and output plain text was completely undecipherable.

## VII. Conclusion

The research work had proposed and implemented a novel cryptography technique that actually is a kind of cryptosystem where two or more ciphering techniques have been combined. In this research the first cipher is affine and second is chaotic neural network. By combining the two approaches together the research work has produced a new ciphering technique involving 4 symmetric keys. The experiment was carried out in octave 4.2.0 and the results were promising. The future research work can be to apply the same hybrid approach to gray and color image encryption and checking performance on large text and images.

## ACKNOWLEDGMENT

The authors would like to thank many researchers and authors whose work have helped us in understanding the research matter well. Special thanks to Google and our colleagues who directly and indirectly helped us in carrying out this research work.

## REFERENCES

[1] Aihara, K., Takabe, T., & Toyoda, M. (1990). Chaotic neural networks. *Physics Letters A, 144*(6–7), 333–340. http://doi.org/10.1016/0375-9601(90)90136-C

[2] Singla, P., Sachdeva, P., & Ahmad, M. (2014). A Chaotic Neural Network Based Cryptographic Pseudo-Random Sequence Design. *2014 Fourth International Conference on Advanced Computing & Communication Technologies*, 301–306. http://doi.org/10.1109/ACCT.2014.38

[3] Lokesh, S., &Kounte, M. R. (2016). Chaotic neural network based pseudo-random sequence generator for cryptographic applications. *Proceedings of the 2015 International Conference on Applied and Theoretical Computing and Communication Technology, ICATccT 2015*, 1–5. http://doi.org/10.1109/ICATCCT.2015.7456845

[4] Abdoun, N., El Assad, S., Taha, M. A., Assaf, R., Deforges, O., & Khalil, M. (2016). Secure Hash Algorithm based on Efficient Chaotic Neural Network. *2016 International Conference on Communications (COMM)*, 405–410. http://doi.org/10.1109/ICComm.2016.7528304

[5] Kaur, H., &Panag, T. S. (2011). Cryptography using chaotic neural network, *4*(2), 417–422. http://doi.org/10.5923/j.ajsp.20140401.04

[6] Kaur, H., &Panag, T. S. (2011). Cryptography using chaotic neural network, *4*(2), 417–422. http://doi.org/10.5923/j.ajsp.20140401.04

[7] Qin, K., &Oommen, B. J. (n.d.). Cryptanalysis of a cryptographic Algorithm that Utilize Chaotic Neural Network, (61300093), 1–8.

[8] Yu, W., & Cao, J. (2006). Cryptography based on delayed chaotic neural networks. *Physics Letters, Section A: General, Atomic and Solid State Physics*, *356*(4–5), 333–338. http://doi.org/10.1016/j.physleta.2006.03.069

[9] Dalkıran, İ., &Danışman, K. (2010). Artificial neural network based chaotic generator for cryptology. *Turk J Elec Eng& Comp Sci*, *18*(2), 225–240. http://doi.org/10.3906/elk-0907-140

[10] Crook, N., & Scheper, T. O. (2001). A Novel Chaotic Neural Network Architecture. *ESANN'2001 Proceedings - European Symposium on Artificial Neural Networks*, (April), 295–300. http://doi.org/10.1109/TNN.2009.2015943

[11] He, Z., Zhang, Y., & Yang, L. (1999). The Study of Chaotic Neural Network and its Applications in Associative Memory. *Neural Processing Letters*, 163–175.

[12] Singh, J., Shyam, P., & Yadav, S. (2014). Implementation of Caesar Cipher and Chaotic Neural network by using MATLAB Simulator, *2*(6), 16–20.

[13] Chauhan, M., & Prajapati, R. (2014). Image Encryption Using Chaotic Cryptosystems and Artificial Neural Network Cryptosystems: A Review, *5*(5), 52–55.

[14] Mhetras, A., &Charniya, N. (2016). Cryptography based on Artificial Neural Networks and Chaos Theory. *International Journal of Computer Applications*, *133*(4), 25–30. http://doi.org/10.5120/ijca2016907743

[15] Jain, A., & Rajpal, N. (2012). Cryptanalysis of a Chaotic Neural Network Based Chaotic Cipher. *Proc. Int. Conf. on Control System and Power Electronics, CSPE*, *333*, 538–544.

## Authors Profile

Dr. Vikas Thada has doctoral and Master's degree in Computer Science & Engineering. He is currently serving as Associate Professor in the Department of Computer Science & Engineering. He has more than 17 years of teaching experience with around 7 years of research experience. He has many publications in international journals and is author of number of books on programming, data structures etc. His research interests genetic algorithm, cryptography, machine learning and deep learning.
.

Mr Utpal Shrivastava has Master's degree in Computer Science & Engineering and pursuing Ph.D in the area of machine learning. He is currently serving as Assistant Professor in the Department of Computer Science & Engineering. He has more than 10 years of teaching experience with around 4 years of research experience. He has many publications in national and international journals. His research interests genetic algorithm, networking, computer graphics and machine learning .