IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Privacy Concern Code Generation Using Crypto Neural Scheme

Anaswara Venunadh[1*], Shruthi N[2], Mannar Mannan[3]

[1] Department of Information Science and Engineering, MVJCE, BANGALORE, India
[2] Department of Information Science and Engineering, MVJCE, BANGALORE,, India
[3] Department of Information Science and Engineering, MVJCE, BANGALORE,, India

[*]*Corresponding Author: anaswara.venunadh@mvjce.edu.in, Tel.: +919902124433*

DOI: https://doi.org/10.26438/ijcse/v7i5.824828 | Available online at: www.ijcseonline.org

Accepted: 18/May/2019, Published: 31/May/2019

***Abstract*—** Frequent imagination by cryptosystem designers that secrets will be manipulated in closed reliable computing environments. Unfortunately, computers and micro systems leak information about the operations they process. This paper examines self-organising neural network to securely transfer data through a given network. We also discuss approaches for building cryptosystems that can operate securely in existing system that leaks.

***Keywords*—**Cryptography, code generation, key management, self-organizing neural networks, encryption, decryption (key words)

I. INTRODUCTION

Cryptography is the study and practice of various techniques for secure communication in the presence of third parties. More generally, it is about constructing and analysing protocols that overcome the influence of attackers or outside people and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Applications of cryptography include ATM cards, computer passwords. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

Cryptography is a field of computer science and mathematics that focuses on techniques for secure communication between two parties while a third-party is present.This is based on methods like encryption, decryption, signing, generating of pseudo random numbers, etc.Nowadays there are in general two different schemes: On the one hand, there are symmetric schemes, where both, sender and receiver, need to have the same key in order to encrypt their communication. For this, they have to securely exchange the key initially. On the other hand, since Diffie and Hellman's key exchange idea from 1976, there also exists the concept of asymmetric schemes where sender and receiver both have a private and a public key. The public key can be shared with anyone, so receiver can use it to encrypt a message for sender. But only sender, with the corresponding private key, can decrypt the encrypted message from receiver. Cryptography plays a very crucial role for private communication through public network. If we have a cryptosystem, the corresponding cipher is given by E resp. D (implicitly also the key spaces K or K ′ resp. κ).There is two main categories of ciphers in terms of key handling: If κ is feasible then K and K ′ need to be kept secret and the cipher is called symmetric. Otherwise the cipher is called asymmetric.

A cryptosystem is a 5-tuple $\Pi := (P ,C ,\kappa,E,D)$ where

1. $P \subset \Sigma 1$, $C \subset \Sigma 2$ • for alphabets $\Sigma 1$,$\Sigma 2$,
2. $\kappa : K' \rightarrow K$ is a bijective map between sets K ,K' ,
3. $E = (Ee)e\in K$ is a family of multivalued maps $Ee : P \rightsquigarrow C$, and
4. $D = (Dd)d\in K'$ is a family of surjective maps $Dd : C$ 7→ P , such that $E\kappa(d) \subset D-1\ d$ for all $d \in K'$ interpreted as multivalued maps.

Such that

$$E\kappa(d) \subset D-1\ d \text{ for all } d \in K'$$

We further require that E and D are realized by polynomial runtime algorithms where E may be probabilistic. Moreover, we call

1. Σ1 the plaintext alphabet and P the set of plaintexts,
2. Σ2 the cipher text alphabet and C the set of cipher texts,
3. K resp. K ′ the encryption resp decryption key space, their elements are called keys and κ is called the key correspondence,
4. E the encryption algorithm resp. Ee the encryption algorithm with key e, and
5. D the decryption algorithm resp. Dd the decryption algorithm with key d.

A neural network is a set of algorithms that try hard to recognize underlying relationships in a set of data through a process that predict the way the human brain operates. Neural networks will adapt to dynamic input that the network generates the most effective potential result without having to revamp the output criteria. The conception of neural networks is fleetly gaining quality within the space of commercialism system development. A "neuron" in a very neural network may be a function that collects and classifies data in keeping with a selected design

A neural network contains layers of interconnected nodes. Each node may be a perception and is comparable to a multiple regression. The perception feeds the signal produced by a multiple linear regression into an activation function that may be nonlinear. Neural networks area unit broadly speaking used, with applications for financial operations, enterprise planning, trading, business analytics and product maintenance. Neural networks have additionally gained widespread adoption in business applications like prediction and market research solutions, fraud detection and risk assessment.

In the rest of this paper Section I contains the introduction of cryptography and neural networks, Section II contain the related work of in the areas of combining cryptography and neural networks, Section III contain the methodology used, Section IV describes results and discussion, Section V concludes research work with future directions.

II. Related Work

Cryptography now referred present day as tools and techniques used to make messages secure for communication between the senders and receivers and make messages protection from possible attacks by hackers. [1]This study presents a novel chaotic-neural network of image encryption and decryption image applied to the domain of medical. The main objective behind the proposed technique is to ensure the safety of medical images with a less complex algorithm compared with the existing methods. In order to improve the robustness, the totality of the pixels related to the host image is XOR with a generation key. After that, with a chaotic system (logistic map), the binary sequence is generated in order to set the weights w_{ij} and bias bi of neuron network with the goal of encrypting the pixels issued from the previous step. Simulation and experiments were carried out on medical images coded on 8 and 12 bits/pixel

[16]Neural cryptography is predicated on synchronization of tree parity machines by mutual learning. We extend previous key-exchange protocols by substitution random inputs with queries looking on the present state of the neural networks. The chance of a productive attack is calculated for various model parameter exploitation numerical simulations. The results show that queries restore the safety against cooperating attackers to gain access private data from user. Thus success chance may be reduced while not increasing the common synchronization time.

III. Methodology

A neural network evaluates worth knowledge and reveals opportunities for creating trade choices supported the information analysis. The networks will distinguish refined nonlinear interdependencies and patterns different ways of technical analysis cannot. However, a ten p.c improvement in potency is all a capitalist will raise from a neural network. There will always be data sets and task classes that a better analyzed by using previously developed algorithms. It is not so much the algorithm that matters; it is the well-prepared input data on the targeted indicator that ultimately determines the level of success of a neural network. Neurons in the visual cortex respond to bars of light. Neurons that answer similar bars are situated next to every different within the cortical region.

Artificial neural networks which are currently used in tasks such as speech and handwriting recognition are based on learning mechanisms in the brain i.e. synaptic changes. In addition, one kind of artificial neural network, self-organizing networks, is based on the topographical organization of the brain. The type of learning utilized in multilayer perceptions requires the correct response to be provided during training (supervised training). Biological systems display this type of learning, but they are also capable of learning by themselves -without a supervisor showing the correct response (unsupervised learning).A neural network with a similar capability is termed a self-organizing system as a result of throughout coaching, the network changes its weights to learn appropriate associations, without any right answers being provided.

In supervised learning, a desired output result for each input vector is required when the network is trained. An ANN of the supervised learning type, such as the multi-layer perceptron, uses the target result to guide the formation of the neural parameters. It is thus possible to make the neural network learn the behaviour of the process under study.

The application of Kohonen networks is typically in mapping very high dimensional input space into 1 or 2 dimensions. Clustering of data sets into distinct groups are used in this group, when you don't know those groups in the beginning. In this technique we are begin with converting the plain text message into their corresponding ASCII values and giving as input to Kohonen network. In Kohonen networks basic units are called neurons and two layers -input layer and the output layer. Input data is presented to the input layer and the values are propagated to output layer. Output layer with a strongest response is said to be the winner.

The application of Kohonen networks is typically in mapping very high dimensional input space into 1 or 2 dimensions. Clustering of data sets into distinct groups are used in this group, when you don't know those groups in the beginning. In this technique we are begin with converting the plain text

message into their corresponding ASCII values and giving as input to Kohonen network. In Kohonen networks basic units are called neurons and two layers -input layer and the output layer. Input data is presented to the input layer and the values are propagated to output layer. Output layer with a strongest response is said to be the winner.

This schema is termed as crypto-neural scheme as a combination of cryptography and neural networks. Common method to compress data is to code them through vector quantization (VQ) techniques [2], [3]. The principle of the VQ techniques is simple. At first, the message is copied into a square block of pixels, for example 4* 4 or 8 * 8; each block is considered as a vector in a 16- or 64-dimensional space, respectively. Second, a limited number of vectors (codeword) in this space is selected in order to approximate as much as possible the distribution of the initial vectors extracted from the square; in other words, more codeword will be placed in the region of the space where there are more points in the initial distribution (image), and vice versa. Third, each vector from the original square is replaced by its nearest codeword (usually according to a second-order distance measure). Finally, in a transmission scheme, the index of the codeword is transmitted instead of the codeword itself; the compression is achieved if the number of bits used to transmit this index ( ) is less than the number of initial bits of the block (if is the resolution of each pixel).

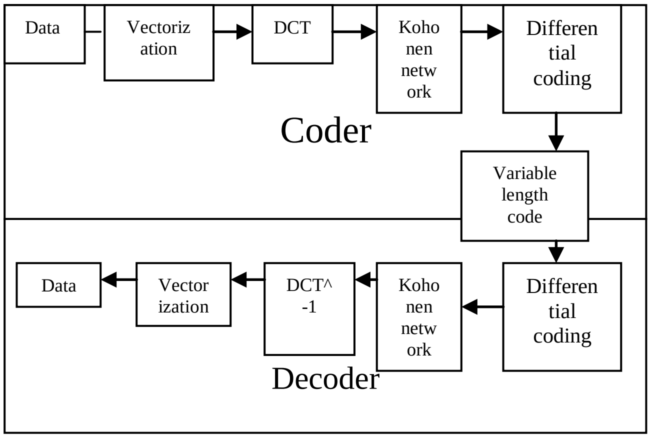

Fig: 1Diagramatic representation of crypto neural scheme

After a vectorization (transformation of data blocks into vectors), a DCT [10] and a low-pass filter first reduce the quantity of information by keeping only the low-frequency coefficients. Then, the vector quantization is performed, with another loss of information. Finally, the indexes of the codeword found by the vector quantize are transformed by a differential coding, and the results are compressed by an entropic coder [11]; these two last steps do not introduce any loss in the information. The decompression scheme performs the same operations in the opposite way

Kohonen’s algorithm has however another important property it realizes a mapping between an input and an output space that preserves topology; in other words, if vectors are near from each other in the input space, their projection in the output space will be close too. In the proposed compression scheme, we will use a two dimensional Kohonen map corresponding to a grid of code words (instead of a one-dimensional table in standard VQ), as the projection of an initial space including all vectors coming from blocks of the initial image.

Differential Coding, if we suppose that particular parts of the message are smooth, a differential coding applied to the code words after vector quantization will lead to “small” codes in average. The main deploy of an entropic coder, is to encode these differences into variable-length words (i.e., words which will take lesser bits if the differences themselves are small), will thus lead to further compression. Because of the entropic coder, the compression ratio will be higher if the difference between code words is low. Instead of using a simple differential scheme (zeroth-order predictor) where each codeword is subtracted from the codeword corresponding to the previously encoded block in the image (i.e., the one at the left of the current block), we will use the following principle (first-order predictor): we suppose that gradients in the image are smooth, and thus that the direction in which the differences between two successive blocks was minimum for already encoded blocks will be the same as the direction in which the difference is minimum for a new block to encode.

IV. Results and Discussion

The main aspect of this paper is to use the topology preserving property of KSOM. According to the selforganization property of KSOM, two consecutive and similar blocks will be coded into similar code words; the use of a differential entropic scheme to encode consecutive blocks will thus improve the compression ratio. An original neural network model is used instead of a first-order predictor. In this paper, we present a compression scheme based on DCT transform of the original message, vector quantization by Kohonen map, differential coding by first-order predictor, and entropic coding of the differences.

For example,
In detail explanation of crypto neural scheme

1. Consider any input which can be a word sentence or any digit.
2. Convert given data into ASCII value (64 bits) and divide into two each of 32 bits.
3. Vectorization-:
   - Data stream divided into (1D or 2D square) blocks -- vectors

- A table or code book is used to find a pattern for each block.
- Code book can be dynamically constructed or predefined.
- Each pattern for block encoded as a look value in table
- Compression achieved as data is effectively sub sampled and coded at this level.

For example:
Load 4 consecutive 32-bit integers (a0, a1, a2, a3)
Load 4 consecutive 32-bit integers (b0, b1, b2, b3)
Perform addition
(c0, c1, c2, c3) ← (a0 + b0, a1 + b1, a2 + b2, a3 + b3)
Store 128-bit vector (c0, c1, c2, c3)

4. Differential cousin transformation.

   Let we are having a 2-D variable named matrix of dimension 8 X 8 which contains image information and a 2-D variable named dct of same dimension which contain the information after applying discrete cosine transform.

   So,

   dct[i][j] = ci * cj (sum(k=0 to m-1) sum(l=0 to n-1) matrix[k][l] * cos((2*k+1) *i*pi/2*m) * cos((2*l+1) *j*pi/2*n)

   where ci= 1/sqrt(m) if i=0 else ci= sqrt(2)/sqrt(m) and

   similarly, cj= 1/sqrt(n) if j=0 else cj= sqrt(2)/sqrt(n) and we have to apply this formula to all the value, i.e., from i=0 to m-1 and j=0 to n-1
5. Differential Encoding

   The difference between the actual value of a sample and a prediction of that values is encoded. Example of technique include: differential pulse code modulation, delta modulation and adaptive pulse code modulation -- differ in prediction part. Suitable where successive signal samples do not differ much, but are not zero.*Differential pulse code modulation* (DPCM) simple prediction:

   $$f_{predict}(t_i) = f_{actual}(t_{i-1})$$
6. After differential encoding variable length code is transferred to receiver side
7. Decoding part follows the reverse path of coder, which will starts with differential decoding, Kohonen network code word comparison, discrete cousin transformation inverse and vector quantization.
8. At decoder side we will receive data as sent with data integrity.

V. Conclusion and Future Scope

In this paper, we proposed a new code generation scheme schema based on the use of the organization property of Kohonen maps. It is based on the fact that consecutive blocks are often similar, and thus coded by similar codeword's with a vector quantization algorithm. The Kohonen map organization property makes the indexes of the coded vectors similar too, and, using an entropy coder, this property is used to increase the security of the message being passed.

Acknowledgment

We thank our colleagues from MVJ College of Engineering who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper.

References

[1] Manel Dridi, Mohamed Ali Hajjaji, Belgacem Bouallegue, Abdellatif Mtibaa Cryptography of medical images based on a combination between chaotic and neural network IET Image processing,volume 10 isssue 11.

[2] Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[3] R. M. Gray, "Vector quantization," IEEE Acoust., Speech, Signal Processing Mag., pp. 9–31, Apr. 1984.

[4] [2] A. Gersho and Robert M. Gray, Vector Quantization and Signal Compression. London: Kluwer, 1992.

[5] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[6] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[7] K. Elissa, "Title of paper if known," unpublished.

[8] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[9] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[10] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.[10] M. Hu, J. Liu, and D. Luo, "Adaptive digital watermarking using neural network techniques", in Proc. Of the 37th Annual Carnahan on intelligent control and Automation, vol. 5, pp. 4066-4069, 2004.

[11] Z. W. N. Wang, and B. Shi, "A novel bind watermarking scheme based on neural network in wavelet domain", in Proc. Of the 6th World Congress on Intelligent Control and Automation, vol. 1, pp. 3024-3027, 2006.

[12] W. Kinzel, and I. Kanter, "Neural Cryptography", in Proc. 9th Int'l Conf. on Neural information Processing (ICONIP'02), vol. 3, pp. 1351-1354,2002.

[13] E. Kilen, R. Mislovaty, I. Kanter, A. Ruttor, and W.Kinzel, "Synchronization of neural network by mutual learning and its application to cryptography", in Proc. NIPS, pp. 689-696, 2004.

[14] R. M. Jogdand, Sahana S. Bisalapur, "Design of an efficient neural key generation", International Journal of Artificial Intelligence and Application (IJAIA), vol. 2, No.1, 60-69, 2011.

[15] Ajit Singh, Aartinandal, "Neural cryptography for secret key exchange and encryption with AES",International Journal of Advanced researched in computer science and software Engineering, vol. 3, issue. 5,376-381,2013.

[16] A. Ruttor, W. Kinzel, I. Kanter, "Neural cryptography with queries", J. stat. Mech., P01009, 2005

Authors Profile

Dr Mannar Mannan pursed Master of Science from Madras University, chennai and Master of Technology in information technologyfrom Bharath Institute of Higher Education, chennai. He pursued Ph.D in Information and Communication Engineering and currently working as Assosiant Professor in Department of Information Science,MVJ College of Engineering since 2018.He has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Information Retrieval,Semantic web,ontology. He has 14 years of teaching experience and 3 years of Research Experience.

Mrs Anaswara Venunadh pursed Bachelor ofTechnology from mahatma gandhi university,kerala and Master of Engineering from Anna University,chennai in year 2013. She is currently working as Assistant Professor in Department of Information Science and Engineering,MVJ College of Engineering since 2015.She has published papers in reputed international journals. Her main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining. She has 3 years of teaching experience.

MRS Shruthi N pursed Bachelor of Engineering from JVIT,Bangalore,Karnataka and Master of Engineering from SJBIT,Bangalore,Karnataka in year 2013. She is currently working as Assistant Professor in Department of Information Science and Engineering,MVJ College of Engineering since 2013.She has published papers in reputed international journals. Her main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy,Computer Networks. She has 3 years of teaching experience.