Crypto - Compression of Medical Images on Neural Cryptography with Queries in Telemedicine System

N. Prabakaran[1], C.M. Velu[2] and P. Vivekanandan[3]

Abstract

There is a requisite to secure the medical images from the hacker admittance when the switch over of medical information is taken place among the patients and doctors. We can generate a private key using neural cryptography, which is based on synchronization of Tree Parity Machines (TPMs) by online learning. The random inputs are generated by Pseudo-Random Number Generators (PRNGs). In the proposed TPMs random inputs are replaced with queries are considered. The queries depend on the current state of A and B TPMs. Then, TPMs hidden layer of each output vectors are compared. That is, the output vectors of hidden unit using Hebbian learning rule, left-dynamic hidden unit using Random walk learning rule and right-dynamic hidden unit using Anti-Hebbian learning rule are compared. Among the compared values, one of the best values is received by the output layer. Similarly, the other hidden units, left-dynamic hidden units and right-dynamic hidden units perform the same operations and values are received by the output layer. A private key (256-bit) with padding bits is used for encryption and decryption in Rijndael algorithm and Huffman coding is used for compression of medical images, which is produced as Crypto-Compressed and Encrypted Medical Images (CCEMI). The CCEMI is protected by password, which is a combination of lower layer's spy unit vector and upper layer's spy unit vector. We have shown more security of medical images, it is very difficult to break a private key by brute force attack.

Keywords: Neural Cryptography, Medical Images, Rijndael algorithm, Crypto-Compression.

1. Introduction

Two identical dynamical systems, starting from different initial conditions can be synchronized by a common input values which are coupled to the two systems. Two networks which are trained on their mutual output can synchronize to a time-dependent state of identical synaptic weights. The networks receive a common input vector after calculating their outputs and update their weight vectors according to the match between their mutual outputs in every time step. The input or output relations are exchanged through a public channel until their weight vectors are identical and can be used as a secret key for encryption and decryption of secret messages. The random inputs are replaced by queries in this network. It is based on exchanging inputs between A and B which are correlated to weight vectors of the two networks [15].

The advancement in computer technology and communication encourages health-care provider to provide health-care over the telemedicine. Telemedicine

[1]Department of Master of Science, St. Peter's University, Avadi, Chennai - 54.

[2] Department of Computer Science and Engineering, SKR Engineering College, Chennai, India.

[3]Director of Knowledge Data Centre, CPDE Building, Anna University, Chennai , India. Email : prabakaran_om@yahoo.com, cmvelu41@gmail.com, vivek@annauniv.edu

is the integration of telecommunications technologies, information technologies, human-machine interface technology and medical care technologies for the purpose of enhancing health delivery across space and time. Telemedicine means the use of computer and communications technologies to augment the delivery of health-care services. Telemedicine can improve access to care, increase health care quality and reduce the cost.

The Rijndael algorithm is used for security of telemedical images and crypto-compression technique is used for reducing the size and decreases the quality of the medical images during the transmission by the networks. The Rijndael algorithm is conventional encryption standard since the common private key (256-bit) is used for encryption and decryption of Discrete Cosine Transform (DCT) coefficients, which is produced as CCEMI.

This paper is organized as follows. In Section 2, the basic algorithm for neural synchronization with queries is given. Also lower layer spy unit, upper layer spy unit, definition of the order parameters and transition probabilities of proposed TPMs are explained. In Section 3, the generation of queries is described. Overview of telemedicine system is briefly explained in Section 4. The crypto-compression technique and Rijndael algorithm of medical images are presented in Sec. 5. In Section 6, the security of medical image is discussed. Finally, conclusion is shown in Section 7.

2. Neural Synchronization

The weight vectors of the two neural networks start with random numbers, which are generated by Pseudo-Random Number Generators (PRNGs) [10]. In these networks, random inputs are replaced by queries. That is A and B choose alternatively according to their own weight vectors. The partners A and B receive a common input vector at each time; their outputs are calculated and then communicated over public channel [12]. If they agree on the mapping between the current input and the output, their weights are updated according to the learning rule.

2.1 A Structure of Tree Parity Machine

The TPMs consist of K-hidden units, Y-left dynamic hidden units and Z-right dynamic hidden units, each of them being a perceptron with an N-dimensional weight vector **w** [4]. The lower layer spy unit (ϑ) is associated with the input units [7]. The upper layer spy unit (ξ) is associated with the hidden units (σ), left-dynamic hidden units (δ), right-dynamic hidden units (γ) and output unit (τ).

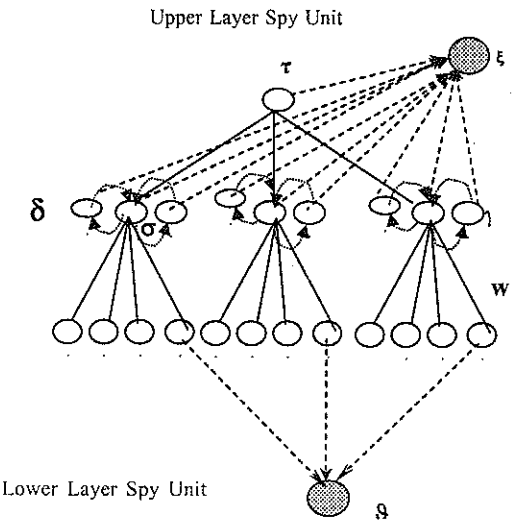


Figure 1: A structure of Tree Parity Machine with K=3, Y=3, Z=3, ϑ=1, ξ=1 and N=4.

The lower layer and upper layer spy units receive the input values from the N-input units, Y-left dynamic hidden units, Z-right dynamic hidden units, K-hidden units and output unit. The network structure of this TPM is shown in Fig.1. The components of the input vectors **x** are binary

$x_{ij} \in \{-1, +1\}, x_{im} \in \{-1, +1\}, x_{ik} \in \{-1, +1\}$ (1)

and the weights are discrete numbers between -L and +L

$$w_{ij} \in \{-L, -L+1, \ldots\ldots, L-1, L\},$$
$$w_{im} \in \{-L, -L+1, \ldots\ldots, L-1, L\},$$
$$w_{ik} \in \{-L, -L+1, \ldots\ldots, L-1, L\}. \quad (2)$$

where L is the depths of the weights of the networks.

The TPM reads the input vectors using queries. These input vectors are correlated with the present weight vector $w_k(t)$. At odd time steps, the partner A generates an input vector which has a certain overlap to its weights w_k^A. At even time steps, the partner B generates an input vector which has a certain overlap to its weights w_k^B. It is based on the queries to improve the security of the systems.

The index i = 1,.....,K denotes the i^{th} hidden unit of TPM , m=1,.....,Y left-dynamic hidden unit of the TPM [6], k=1,.....,Z right-dynamic hidden unit of the TPM and j =1,....,N denotes the N input units.

The different transfer functions for hidden layer are given below

$$\sigma_i = \operatorname{sign}\left(\sum_{j=1}^{N} w_{ij} \circ x_{ij}\right) \quad (3)$$

$$\delta_i = \tanh\left(\sum_{m=1}^{N} w_{im} \circ x_{im}\right) \quad (4)$$

$$\gamma_i = \arctan\left(\sum_{k=1}^{N} w_{ik} \circ x_{ik}\right) \quad (5)$$

where equation (3) is the transfer function of the hidden unit, the equation (4) the transfer function of the left-dynamic hidden unit and the equation (5) the transfer function of the right-dynamic hidden unit.

The transfer functions for lower layer spy unit and upper layer spy unit are given below

$$\vartheta = -\operatorname{sign}\left(\sum_{i=1}^{N}\left[\sum_{j=1}^{N} x_{ij}\, g w_{ij}\right]\right) \quad (6)$$

$$\xi = -\operatorname{sign}\left(\sum_{i=1}^{K} \delta_i\ \sigma_i \gamma_i\ \tau\right) \quad (7)$$

where the equation (6) is the transfer function of the lower layer spy unit and equation (7) the transfer function of the upper layer spy unit.

The K-hidden units of σ_i, Y-left dynamic hidden units of δ_i and Z-right dynamic hidden units of γ_i define common output bit of hidden layer of the network and are given by

$$\beta_a = \prod_{i=1}^{K} \sigma_i \quad (8)$$

$$\beta_b = \prod_{i=1}^{Y} \delta_i \quad (9)$$

$$\beta_c = \prod_{i=1}^{Z} \gamma_i \quad (10)$$

where equation (8) is the output for the hidden units, equation (9) the output for the left-dynamic hidden units and equation (10) the output for the right-dynamic hidden units.

The two TPMs compare the hidden layer's output bits (hidden, left-dynamic and right-dynamic hidden units) and then update the weight vector to the output unit as well as partners A and B that are trying to synchronize their weight vectors [8].

$$\psi_i^{A,B} = comp(\beta_a, \beta_b, \beta_c) \quad (11)$$

$$\phi_i^A = w_{ij}^A\ x_{ij}^A\ \tau^B \psi_i^A \quad (12)$$

$$\phi_i^B = w_{ij}^B\ x_{ij}^B\ \tau^A \psi_i^B \quad (13)$$

where equation (11) represents comparison of the output of hidden, left-dynamic and right-dynamic hidden units of A and B. The equation (12) and (13) represent output of hidden, left and right-dynamic hidden units of A and B respectively.

$$\tau = \prod_{i=1}^{K} \phi_i \qquad (14)$$

The equation (14) represents the output vector of the output unit of the TPM.

2.2 Learning Rules

The partners A and B initialize their random number of weight vectors before the start of the training period. At each time step t, a public input vector is generated and the bits τ^A and τ^B are switched over the public channel. In the case of indistinguishable output bits $\tau^A = \tau^B$, each TPM adjust those of its weight vectors for which the hidden unit, left-dynamic hidden unit and right-dynamic hidden unit is identical to the output $\phi^{A/B} = \tau^{A/B}$. These weights are adjusted according to a given learning rules. They are

(a) Hebbian Learning rule for hidden units

$$w_i^A(t+1) = w_i^A(t) + x_i \tau^A \Theta(\tau^A \phi_i^A)\Theta(\tau^A \tau^B)$$
$$w_i^B(t+1) = w_i^B(t) + x_i \tau^B \Theta(\tau^B \phi_i^B)\Theta(\tau^A \tau^B) \qquad (15)$$

where Θ is the Heaviside step function, if the input is positive then the output is 1 and if input is negative then the function evaluates to 0.

(b) Random walk learning for left-dynamic hidden units

$$w_i^A(t+1) = w_i^A(t) + x_i \Theta(\tau^A \phi_i^A)\Theta(\tau^A \tau^B)$$
$$w_i^B(t+1) = w_i^B(t) + x_i \Theta(\tau^B \phi_i^B)\Theta(\tau^A \tau^B) \qquad (16)$$

(c) Anti-Hebbian learning for right-dynamic hidden units

$$w_i^A(t+1) = w_i^A(t) - \tau^A x_i \Theta(\tau^A \phi_i^A)\Theta(\tau^A \tau^B)$$
$$w_i^B(t+1) = w_i^B(t) - \tau^B x_i \Theta(\tau^B \phi_i^B)\Theta(\tau^A \tau^B) \qquad (17)$$

2.3 Order Parameters

The process of synchronization itself can be described by standard order parameters. These order parameters are

$$Q_i = \frac{W_i^A \cdot W_i^A}{N}, Q_j = \frac{W_j^A \cdot W_j^A}{N}, Q_k = \frac{W_k^A \cdot W_k^A}{N} \qquad (18)$$

The equation (18) represents weight distribution of hidden units, left-dynamic hidden units and right-dynamic hidden units of A's TPM.

$$R_i^{A,B} = \frac{W_i^A \cdot W_i^B}{N}, R_j^{A,B} = \frac{W_j^A \cdot W_j^B}{N}, R_k^{A,B} = \frac{W_k^A \cdot W_k^B}{N} \qquad (19)$$

The equation (19) represents overlap between two hidden units, two left-dynamic hidden units and two right-dynamic hidden units of A and B respectively.

The distance between two corresponding hidden unit, left-dynamic hidden units and right-dynamic hidden units are defined by the overlap is given below

$$\rho_{ijk}^{A,B} = \frac{R_i^{A,B}}{\sqrt{Q_i^A Q_i^B}} + \frac{R_j^{A,B}}{\sqrt{Q_j^A Q_j^B}} + \frac{R_k^{A,B}}{\sqrt{Q_k^A Q_k^B}} \qquad (20)$$

2.4 Transition Probabilities

A repulsive step can only occur in the i^{th} hidden unit, j^{th} left-dynamic hidden unit and k^{th} right-dynamic hidden unit, if the two corresponding outputs ϕ_i are different. The probability for this event is given by the well-known generalization error for the perceptron [13]

$$\varepsilon_p^{ijk} = \frac{1}{\pi} \arccos(\rho_{ijk}) \qquad (21)$$

where equation (21) represents the generalization error for hidden, left-dynamic and right-dynamic unit of two TPMs.

The quantity ε_p^{ijk} is a measure of the distance between the weight vectors of the corresponding hidden units, left-dynamic hidden units and right-dynamic hidden units these values are independent. The values ε_p^{ijk} determine the conditional probability P_r for a repulsive step and P_a for a attractive step between two hidden units, left-dynamic hidden units and right-dynamic hidden units given identical output bits of the two TPMs. In the case

of identical distances $\varepsilon_\rho^{ijk} = \varepsilon$, the values of K, Y, and Z are found as K=3, Y=3 and Z=3.

$$P_a^B = \frac{1}{2}\frac{(1-\varepsilon)^3 + 3(1-\varepsilon)\varepsilon^2}{(1-\varepsilon)^3 + 9(1-\varepsilon)\varepsilon^2} \quad (22)$$

$$P_r^B = \frac{6(1-\varepsilon)\ \varepsilon^2}{3(1-\varepsilon)^3 + 9(1-\varepsilon)\varepsilon^2} \quad (23)$$

The equation (22) and (23) represent probability of attractive and repulsive steps between two hidden units, two left-dynamic hidden units and two right-dynamic hidden units of A and B respectively.

The attacker E can assign a confidence level to each output σ_i^E, δ_i^E *and* γ_i^E of its hidden units, left-dynamic hidden units and right-dynamic hidden units. For this task the local field is given by

$$h_{ijk} = \frac{w_i \cdot x_i}{\sqrt{N}} + \frac{w_j \cdot x_j}{\sqrt{N}} + \frac{w_k \cdot x_k}{\sqrt{N}} \quad (24)$$

where equation (24) represents the local field of hidden unit, left-dynamic and right-dynamic hidden units of an attacker's TPM.

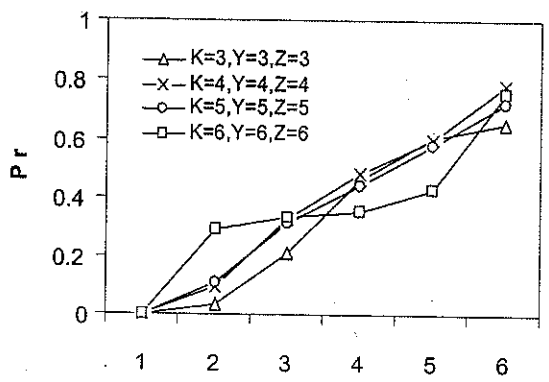


Figure 2 : Probability $P_r^B(\rho)$ of repulsive steps for synchronization with mutual interaction under the condition $\tau^A = \tau^B$.

From the above fig. 2, we are able to predict the probability of repulsive steps occur more frequently in E's TPM than in A's and B's for equal overlap $0 < \rho < 1$. So, the partners A and B have a clear advantage over a simple attack in neural cryptography.

Then the prediction error the probability of different output bits for an input vectors 'x' inducing a local field h_{ijk} is given below [14]

$$\varepsilon(\rho_{ijk}, h_{ijk}) = \frac{1}{2}\left[1 - erf\left(\frac{\rho_{ijk}}{\sqrt{2(1-\rho_{ijk}^2)}}\frac{|h_{ijk}|}{\sqrt{Q_i}}\right)\right] \quad (25)$$

where equation (25) represents prediction error of the local field of hidden units, left-dynamic and right-dynamic hidden units of an attacker's TPM.

3. Generation Of Queries

As both inputs $x_{i,m}$ and weights $w_{i,m}$ are discrete, there are only (2L+1) possible solutions for the product $x_{i,m} \cdot w_{i,m}$ [11]. Therefore, a set of input vectors consisting of all permutation, which do not exchange h_i, can be depicted by counting the number $c_{i,l}$ of products with $x_{i,m} \cdot w_{i,m} = l$. Then the local field is given by

$$h_{ijk} = \frac{1}{\sqrt{N}}\left[\sum_{l=1}^{L}\left(l(c_{i,l} - c_{i,-l}) + l(c_{j,l} - c_{j,-l}) + l(c_{k,l} - c_{k,-l})\right)\right] \quad (26)$$

where equation (26) is the number of inputs and weights in the local field of TPM.

The sum $n_{ijk,l} = c_{i,l} + c_{i,-l} + c_{j,l} + c_{j,-l} + c_{k,l} + c_{k,-l}$ is equal to the number of weights with $|w_{i,j}| = |l|$ and thus independent of 'x'. Accordingly, one can write h_{ijk} as a function of only L variables, because the generation of queries cannot change 'w'.

$$h_{ijk} = \frac{1}{\sqrt{N}}\left[\sum_{l=1}^{L}\left(l(2c_{i,l} - n_{i,l}) + l(2c_{j,l} - n_{j,l}) + l(2c_{k,l} - n_{k,l})\right)\right] \quad (27)$$

where equation (27) is the inputs and sum of current weights vectors of the local field of two TPMs.

The inputs vectors 'x' is connected with zero weights which are selected by randomly, because they do not determine the local field. The other input bits $x_{i,m}$ are divided into L groups according to the absolute value $l = |w_{i,m}|$ of their corresponding weight. In each group, $c_{i,l}$ inputs are selected randomly and set to $x_{i,m}$=sign($w_{i,m}$). The remaining $n_{i,l} - c_{i,l}$ input bits are set to $x_{i,m}$ = -sign ($w_{i,m}$).

The maximum possibilities of the weight vectors of an attacker's TPM is given by

$$l_{\max} = (4L+2)^{(K+Y+Z)\cdot N} \qquad (28)$$

Then

$$\ln (l_{\max}) = (K+Y+Z)\cdot N \ln(4L+2) \qquad (29)$$

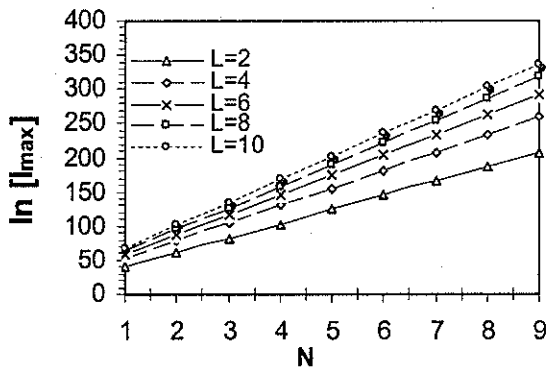


Figure 3: The Possible Values Of L_{max} Of The Weight Vectors Of An Attack's TPM.

From the above fig.3, we are able to determine a large number of possibilities of weight vectors against an attacker, in which weights are selected by queries. In each time step, either A or B generates the input vectors. The attacker E cannot easily gain the weight vector and useful information from analyzing queries.

4. Overview Of Telemedicine System

The rapidly evolving telecommunications technologies are creating an environment where individuals will be able to communicate interactively using a variety of media. The application of these technologies to provide medical care is referred to as telemedicine. The medical images for these new technologies is being researched, but it is still to be determined how effective these technologies will be in extending the reach of medical care to geographically and socio-economically isolated populations.

Despite an abundance of physicians and a large, well financed health care system, many areas of the United States still face a chronic shortage of medical providers of all types. Additionally, the ability of most persons living in rural areas to receive the most current specialty or sub-specialty care will be limited geographically under any future system of health care envisioned. These access and provider distribution issues must be addressed in order to achieve quality health care in the medically sub-urban area. The ability to provide medical care through telemedicine offers a practical solution to this misdistribution.

Telemedicine is the use of electronic communication and information technologies to provide clinical services when participants are at different locations. Videoconferencing, transmission of telemedical images, e-health including patient portals, remote monitoring of vital signs, continuing medical education and nursing call centers are all considered part of telemedicine and tele-health. Telemedicine offers a means to help transform healthcare itself by encouraging greater consumes involvement in decision making and providing new approaches to maintaining a health lifestyle.

5. Crypto - Compression of Medical Image

The medical image is grouped into 8x8 blocks, changed from unsigned integers to signed integer and input to the Forward DCT (FDCT). At the output from the decoder, the inverse DCT outputs 8x8 sample blocks to

form the reconstructed image. Then, each DCT coefficients is separated by its corresponding constant in a standard quantization table and succeeded by rounding to the closest integer. This output value is normalized by the quantizer step size. Dequantization is the inverse function which returns the result to a representation appropriate for input to the IDCT [2]. All of the quantized coefficients are ordered into the 'zig-zag' sequence. This ordering helps to facilitate entropy coding by placing low-frequency coefficients before high-frequency coefficients.

The medical images, which specifies entropy coding method is Huffman coding. The 2-step process of entropy encoding converts the zig-zag sequence of quantized coefficients into an intermediate sequence of symbols and converts the symbols to a data stream in which the symbols no longer have externally identifiable boundaries.

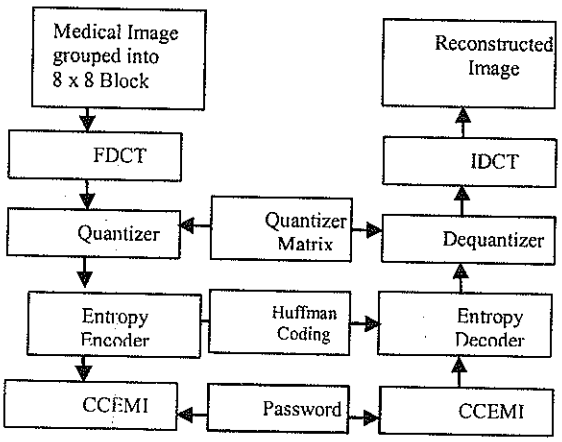


Figure 4 : DCT-Based Encoder and Decoder processing Steps of CCEMI

In each block, the 64 DCT coefficients are arranged from the lowest (upper left corner) to the highest frequencies (lower right corner). The most significant visual characteristics of the images are located in the low frequencies while the particulars are situated in the higher frequencies. The HVS (Human Visual system) is very sensitive to lower frequencies than to higher ones [9].

The Rijndael algorithm reads the input of medical image data block from the FDCT coefficients and execute various transformations for encryption and decryption. These are constituted as two-dimensional array of bytes [9]. The total number of rounds is 24 for encryption and decryption of medical image of FDCT coefficients block using private key which is generated by two TPMs. To encrypt a block of medical image of FDCT coefficients in AES (Advanced Encryption Standard), we first perform an Add Round Key step (XORing a sub-key with the block) by itself. There are regular rounds that involve 4 steps

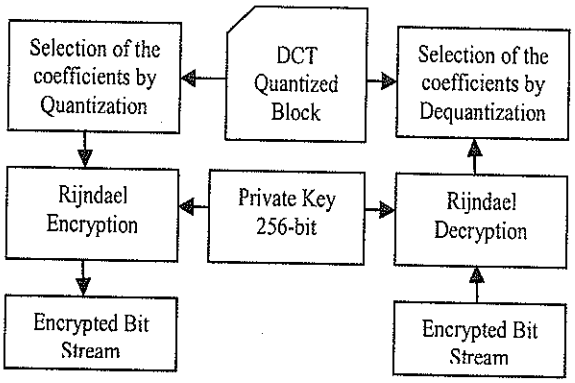


Figure 5 : Rijndael Encryption and Decryption processing steps of FDCT and IDCT Coefficients

(i) Add Round Key Transformation

A Round key is summed to the state by a simple bitwise XOR operation with compound of the expanded private key [16].

(ii) SubBytes Transformation

The SubBytes transformation is a non-linear byte substitution that operates independently on each byte of the state using a substitution table (S-Box), which is invertible, is constructed by composing two transformations:

1. The multiplicative inverse in the Galois Field (2^8) with the irreducible polynomial is $m(x) = x^8 + x^4 + x^3 + x + 1$. The element {00} is mapped to itself.

2. Apply the affine transformation (over GF(2^8)):

The inverse of SubBytes transformation which is needed for decryption, is the inverse of the affine transformation followed by the same inversion as the SubBytes transformation

(iii) ShiftRows Transformation

The ShiftRows transformation rotates each row of the input state to the left shift and then offset of the rotation corresponds to the row number. The inverse of this transformation is computed by performing the corresponding rotations to the right shift.

(iv) Mixcolumns Transformation

The Mixcolumns transformation operates on the state column-by-column, treating each column as a four-term polynomial. The columns are considered as polynomial over GF (2^8) and multiplied modulo $(x^4 + 1)$ with a fixed polynomial a(x), given by

$$a(x) = \{03\} x^3 + \{01\} x^2 + \{01\} x + \{02\} \quad (30)$$

The coefficient of a(x) is also elements of GF(2^8) and is represented by the hexadecimal values in this equation. The inverse mixcolumn transformation is the multiplication of each column with

$$a^{-1}(x) = \{0B\} x^3 + \{0D\} x^2 + \{09\} x + \{0E\} \quad (31)$$

modulo (x^4+1) for decryption process.

6. The Security Of Medical Images

Here, we determine that queries to increase the security of the neural key-exchange protocol and synchronization time. The CCEMI is based on the password-protection with padding bits, which is a combination of lower layer's spy unit vector and upper layer's spy unit vector. The medical images are encrypted and decrypted using 256-bit private key in Rijndael algorithm and compressed with Huffman coding. If the attacker wants to break the password then he has to decode the CCEMI and decrypt using 256-bit private key. An attacker tries to find out all possibilities 1.16×10^{77} of the right key. The attacker will take 10^{56} years to break the secret key using brute force attack.

7. Conclusion

In the proposed TPMs, we trained the three transfer functions in the hidden layer. That is, hidden unit using Hebbian learning rule, left-dynamic hidden unit using Random walk rule and right-dynamic hidden unit using Anti-Hebbian learning rule included with queries. Also, the queries increase the probability of repulsive steps for an attacker during the synchronization. In addition, the method receives a new parameter, which can be adapted to give optimal security. The CCEMI has more secured due to password-protection, crypto-compression using Huffman coding and private key (256-bit) in Rijndael encryption. A private key is generated by two TPMs. The CCEMI reduces the time for transmission and the space on disk. For the attacker to find out all possibilities of password keys and private keys, it will take trillion years against the brute force attack.

References

[1] Engel A and Van Den Broeck C, *"Statistical Mechanics of Learning"*, Cambridge University Press, Cambridge, 2001.

[2] Gergory K. Wallace, *"The JPEG Still Picture Compression Standard"*, ACM, Apr 1991.

[3] Jean-Claude Borie, William Puech and Michel Dumas, *"Crypto-compression system for secure transfer of medical images"*, University of Montpeillier II, France.

[4] Kinzel W and Kanter I, *"Interacting neural networks and cryptography"*, Advances in Solid State Physics, by B. Kramer (Springer, Berlin) Vol. 42, PP.383-391, 2002. [cond-mat/0203011].

[5] Penrose. A.J, Neil A. Dodgson, *"Extending Lossless Image Compression"*, Euro graphics UK'99, Fitzwilliam College, Cambridge, PP. 13-15, Apr 1999.

[6] Prabakaran N, Loganathan P and Vivekanandan. P, *"Neural Cryptography with Multiple Transfer function and Multiple Learning Rule"*, International Journal of Soft Computing, Vol. 3 (3), P.P. 177-181, 2008.

[7] Prabakaran N, Karuppuchamy P and Vivekanandan P, *"A New approach on Neural Cryptography with Dynamic and Spy units using multiple transfer functions and learning rules"*, Asian Journal of Information Technology, Accepted, 2008.

[8] Prabakaran N, Saravanan P and Vivekanandan P, *"A New technique on Neural Cryptography with Securing of Electronic Medical Records in Telemedicine System"*, International Journal of Soft Computing, Vol. 3 (5), PP. 390-396, 2008.

[9] Puech W, Rodrigues. J.M, *"Crypto-Compression of Medical Images by selective encryption of DCT"*, University of Motpeillier II, France.

[10] Ruttor A, Kinzel W, Shacham L and Kanter I, *"Neural cryptography with feedback"*, Physical Review E, Vol. 69, PP.1-8, 2004.

[11] Ruttor A, *"Neural Synchronization and Cryptography"*, Ph. D. Thesis, 2006.

[12] Ruttor A, Kinzel W and Kanter I, *"Neural cryptography with queries"*, In: Physics Rev. E. Vol. 25, No. 01, PP.01-12, 2002.

[13] Ruttor A, Kanter I and Kinzel W, *"Dynamics of neural cryptography"*, [cont-mat/061257/ 21 Dec 2006].

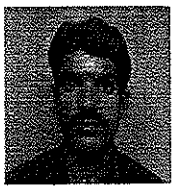
[14] Ruttor A, Kanter I, Naeh R and Kinzel W, *"Genetic attack on neural cryptography"*, [cond-mat/ 0512022v2/1 Jun 2006].

[15] Rachel Mislovaty, Einat Klein, Ido Kanter and Wolfgang Kinzel, *"Public channel cryptography by synchronization of neural networks and chaotic maps"* [cond-mat/0302097 Vol.1, 5 Feb 2003].

[16] Sharma S and T.S.B. Sudarshan T.S.B, *"Design of an efficient architecture for advanced encryption standard algorithm using systolic structures"*, International Conference of High Performance Computing (HiPC), 2005.

Author's Biography

Vivekanandan Periyasamy received his Master of Science in Applied Mathematics from Madras University in 1978 and Doctor of Philosophy from Anna University in 1987. Also, he obtained his postgraduate degree in Master of Engineering in Computer Science and Engineering from Anna University in 1995. He is working as Professor of Mathematics, Department of Mathematics in Anna University from 1978. He visited Singapore, Malaysia, Bangladesh, Sultanate of Oman, Thailand, JAPAN and USA three times for presenting research papers and Chairing Sessions. He has published more than 77 research papers in national and international journals. His areas of research are Neural Networks, Internet Security and Software Reliability. Also, he is Director, KNowledge Data Centre, CPDE Building, Anna University, Chennai-600 025, India.



Prabakaran N , received M.Sc in Computer Science from Anna University. He is doing research under the research under the guidance of Dr. P. Vivekanandan. His areas of interest are network security, visual programming, computer networks, neural networks and c# programming. He had published seven papers in International Journals and four papers in international conferences.

C. M. VELU received his Master of Science in Operations Research and Statistical Quality Control from Sri Venkateswara University, Tirupathi in 1985 and M.S in Computer Systems and Information from BITS, PILANI in 1994. He is currently doing research in Computer Science in Anna University under the guidance of Dr.P.Vivekanandan. He has visited UAE as a Computer faculty. He served as faculty of Computer Science and Engineering for more than two decades. He has published seven research papers in international journals. His areas of research are Artificial Neural Network, Digital Image Processing, Pattern Recognition, Data Compression, Data Warehousing and Data Mining. He has published about five papers in national and international conferences.