VOL. 11, NO. 1, JANUARY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A SECURE IMAGE ENCRYPTION ALGORITHM BASED ON ANN AND RUBIK'S CUBE PRINCIPLE

T. Gomathi[1] and B. L. Shivakumar[2]
[1]Department of Computer Science, Karpagam University, Coimbatore, India
[2]Department of Computer Applications, Sri Ramakrishna Engineering College, Coimbatore, India
E-Mail: gomatisabari@gmail.com

ABSTRACT

Steganography is the science of concealing the information. The text data or an image in one format is being hidden by another image or text data of the same or of the different format. Nowadays data transmitted are being hacked by meddler; in order to avoid hacking the data is transmitted in several ways of techniques such as encryption, scrambling, watermarking and steganography. Although steganography is used to protect information from unwanted parties; the strength of steganography can be amplified by combining it with cryptography. In this paper a new method called ANN based multistage image encryption using Rubik's cube method is proposed for secured data transmission.

Keywords: encryption, HVS (Human Visual System), LSB (Least Significant Bit), PSNR (Peak Signal Noise Ratio), steganography, Rubik's cube algorithm, NPCR (Number of Pixel Change Ratio) ANN (Artificial Neural Network).

1. INTRODUCTION

In this digital era, computers and the internet are major communication media. They connect different parts of the world and have made the world one global virtual world. As a result, people can easily exchange information without distance being a hindrance. At same time, the recent growth of computer power and storage, the difficulties in ensuring individual's privacy become increasingly challenging. The degrees to which individuals appreciate privacy differ from one person to another. In the recent past, various methods have been investigated and developed to protect personal privacy. Encryption is probably the most obvious one, and then comes steganography. The similarity between steganography and cryptography is that, both are used to conceal information. But the difference is that the steganography does not reveal any suspicious about the hidden information to the user. Therefore the attackers will not try to decrypt information. The term steganography is retrieved from the Greek words stegos means cover and grafia meaning writing defining it as covered writing [1].

The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information [2]. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

Steganography is the art of covered or hidden writing. In an image Steganography the information is hidden exclusively in images. Steganography techniques can be applied to images, a video file or an audio file. Typically, steganography is written in characters including hash marking, but its usage within images is also common. Steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing. Even though Steganography is a way to protect information from unwanted parties, the strength of steganography can be amplified by combining it with cryptography. The technique of steganography can be explained using the following block diagram [3].

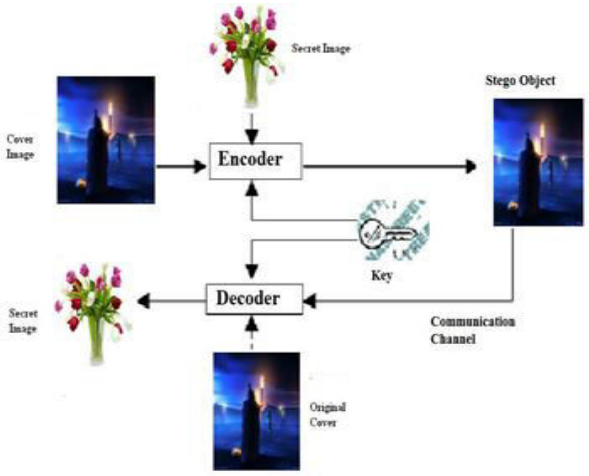

Figure-1. Block diagram of Steganography.

In this diagram, the secret image is covered or hidden within the cover image and it is given has input, and it is encoded or encrypted as Stego image and this image is sent through by communication channel. Using the secret key, which is known only to the sender and the receiver, then stego image is again decoded or de-encrypted, finally secret image is recovered from the cover image. This reduces the risk of hacking data or third party attacks.

ANN is computation model derived from a human brain and its nervous system. ANN is a machine learning method used as artificial intelligence which can needed where non-linear conditions apply. For example a dataset x= [1 4 6 8 100 103] as input and t= [2 8 12 16 200 206] as output of the system then it is possible to give a relation and expect or predict the output of system when Input is given. This example show above is a linear system and AI like Fuzzy and ANN is not needed. Whereas for input x= [1 4 8 100 201 44 4 8 68 89] the output given y= [5 6 78 53 6 9 0 99 89] it not possible to give an exact relation and cannot expect a precise output. To overcome the above non-linearity and to map the input and output the ANN is used. Also another example to explain this is recognizing the handwriting of different persons which is possible to do by human brain and not by machines without AI (Artificial Intelligence).Usually human brain has a property such as it is**(1)adaptive** to the different systems and process. When human wants to drive a vehicle, brain automatically remembers and implements all the rules and methods to drive a vehicle. While working in computer his/her brain uses all the knowledge he/she has gained all those past years. He remembers all the shortcuts, where his personal folder is located etc. **(2)Input output mapping**- from the child hood our brain is trained to map certain thing. For example a baby is taught to recognize flowers, for that some flower samples are show to it like ‘rose’, ‘lotus’. After the training when ‘lily’ is shown and asked to recognize then the answer will be flower. The baby cannot precisely say it is lily flower but it can say it is flower. Likewise a cat is show and asked to recognize it then the baby cannot recognize the object shown, its answer will be “it is not a flower” due to insufficient data training. **(3)Massively parallel Computation-** the human brain has the capability doing things parallelly. For example let’s take teachers who take classes in school or college, while teaching classes certain things will be processed parallely in their brain. While teaching some concepts to the students they parallely think is going to teach next, the students are listening or not, is it anyone looking him to ask doubts, control over words he spoke, his body language, a sudden real time example for concepts he teaching. Another example is while driving vehicle our brain will parallely processes the road rules, speed limit given, thinking of gear level suitable to that particular road, steering angle required to cross the road curve etc. This massively parallel processing methodology makes our human brain faster than even our modern computers. **(4)Non linearity-** non linearity is another important property of brain in which always finds the relation between samples given, for example today we have lot of advanced forecasting system to give information about rain and weather condition. But some trained brains especially farmers can able to predict whether it rains or not [4].

To overcome the non-linearity and to map the input and output, the ANN (Artificial Neural Network) is used. Also another example to explain this is, recognizing the handwriting of different persons which is possible to do by human brain and not by machines without AI (Artificial Intelligence). The details about how this biological model of brain and nerves system is converted to mathematical model .A structure of typical neuron consists of nucleus located inside a cell body has axon attached to it. At the end of this axon the synaptic which is end terminal like structure is present. The end terminal in a cell body is known as dendrites are present. The reason for explaining these biological structures is to explain how this formation of methodology is used in ANN mathematical model. This biological setup is knows a neurons in which dendrites.

The neural network consists of 3 layers to manipulate the training they are Input Layer, Hidden layer and an Output layer which is formed with the replication of the biological model ANN has the ability to acquire knowledge from its surrounding by their internal parameter adaptation. It has adaptive learning technique for finding out the relationship among different example, without requiring previous model. Self-organization is one of the properties of ANN for distribute information to entire network; there is no element with specific storage information [5].

This paper is organized, where Section II describes some of the popular encryption methods. And the proposed method is Artificial Neural Network (**ANN)** based on Multistage Image Encryption using Rubik’s Magic cube method is given in section III and the experimental results of the proposed method are discussed in Section IV followed by conclusion in Section V.

2. SOME OF THE POPULAR ENCRYPTION METHODS

i) Data encryption standard: DES is a block cipher meaning it operates on plaintext blocks of a given size (64-bits) and returns cipher text blocks of the same size. Thus DES results in a permutation among the 2^64 (read this as: "2 to the 64th power") possible arrangements of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block **L** and a right half **R**. (This division is only used in certain operations.)

ii) Block based standards: The block based standards for encrypting involves converting the image into smaller blocks and transferring them into another form. These transferred blocks are again replaced in the same location. Since the entire process takes places only in terms of blocks the encrypted image consists of patterns with difference between each block in the image.

iii) Rubik's cube method: This algorithm contains image of six blocks which had six faces of a cube and then shuffling of the cube takes place. Because of this shuffling of faces the positions of the pixels gets changed. This process when applied in reverse will result in original data. Thus the security level in this method is less.

iv) Enigmaintermix cube encryption: Enigma Intermix cube method is used for Encryption where the key letter can be any character such that it must have an ASCII value. That key value is always confidential between the sender and the receiver. The intruder can't guess that an XOR operation is being done and if known the key will be unknown. The entire image I_0 is divided into 9x6 blocks. The pixels in each block are shuffled based on Rubik's Cube method. Let I_0 represents a gray scale image of size M x N. Here M=9 and N=6.Here I_0 represent the pixels values matrix of image I.

v) LSBtechnique algorithm: The encrypted image cannot be send as such to the receiver since it may be hacked by the intruders so the encrypted image is next put into a process of steganography. The method used to hide the message image is LSB algorithm.

Step 1: The encrypted image is now converted into binary form such that each pixel value contains 8 bits of value.

Step 2: After converting the encrypted image into binary values it is split into LSB and MSB values.

Step 3: Cover image is also converted into binary values each comprising of 8 bits.

Step 4: After converting the cover image into binary values it is also split into LSB and MSB values.

Step 5: After the splitting process the MSB of Encrypted image is now combined with MSB of cover image. (i.e.) the LSB of cover image is replaced with MSB of Encrypted image.

Step 6: This process is repeated to all pixels in the Cover image and a new set of pixels values is obtained.

Step 7: Finally convert the binary values into integers and thus it forms the stegano image.

3. PROPOSED METHODOLOGY

Steganography is done in several ways like hiding text in image, audio in image or image behind image. This work implements a new method for hiding image behind image. The method in order to have a secure transmission with no data loss uses a new method called ANN based Rubik's cube principle. This involves the following steps.

a) Image Importing
b) Pre-processing image
c) Generate Public Key and Private Key
d) Regression Neural Network
e) Linear Regression
f) Key Based Encrypting Image
a. 7 Constructing stegano image
b. 8 Transmitting data
c. 9 Reconstructing Stegano image
d. 10 Key based decrypting image

A. Image importing: The data chosen in this method is an image. The image to be hidden and the image which is to hide the secret image are to be chosen. The image chosen are true colorRGB images and are processed as such. The format of an RGB image could be in png, jpeg, tiff, etc,

B. Pre-processing image: Basically several images will not be of good quality, perfect size or with good brightness and contrast. Such images when taken for further processing may result unexpectedly. So every image should be enhanced in terms of quality and resized properly. Two Resizing process are done here.

a) The secret image is resized to a size of A x A (for ex, A=128).
b) The cover image is resized to a size of 2A x 2A (for ex, when A=128, 2A=2*128=256).

C. Generate public key and private key: Public-key refers to a cryptographic mechanism. It has been named public-key to differentiate it from the traditional and more intuitive cryptographic mechanism known as: symmetric-key, shared secret, secret-key and also called private-key.

Symmetric-key cryptography is a mechanism by which the same key is used for both encrypting and decrypting; it is more intuitive because of its similarity of locking and unlocking a door: the same key. This characteristic requires sophisticated mechanisms to securely distribute the secret-key to both parties. Public-key on the other hand, introduces another concept involving key pairs: one for encrypting, the other for decrypting. This concept, which explained below is very clever and attractive, and provides a great deal of advantages over symmetric-key:

- Simplified key distribution
- Digital Signature

- Long term expression

Public-key is commonly used to identify a cryptographic method that uses an asymmetric-key pair (a public-key and a private-key). Public-key encryption uses that key pair for encryption and decryption. The public-key is made public and is distributed widely and freely. The private-key is never distributed and must be kept secret. Given a key pair, data encrypted with the public-key can only be decrypted with its private key; conversely, data encrypted with the private-key can only be decrypted with its public key. This characteristic is used to implement encryption and digital signature.

D. Regression neural network: Regression is a process for estimating the relationships between variables. It involves many techniques for modeling and analyzing several variables. Regression analysis estimates the average value of the dependent variables by keeping the independent values fixed. Estimated target is the function of independent values which is also named as regression function. Regression analysis is mainly used for forecasting and prediction.

Regression is of two basic types they are

a) Parametric regression
b) Nonparametric regression

Parametric regression refers to the technique that involves a finite number of unknown parameters that are estimated from the data and Nonparametric regression refers to techniques that allow the regression function to lie in a specified set of functions, which may be infinite-dimensional. Linear regression, ordinary least square regression are some of the parametric regression and nonlinear regression is a nonparametric regression.

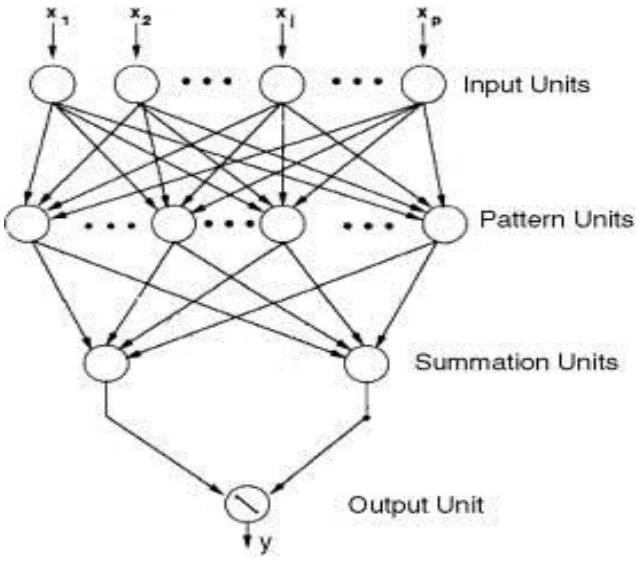

Figure-2. General regression neural network.

E. Linear regression: Linear regression is an approach to model the relationship between a scalar dependent variable y and one or more explanatory variables denoted x. The case of one explanatory variable is called simple linear regression. In linear regression, data are modeled using linear predictor functions, and unknown model parameters are estimated from the data. Such models are called linear models. Most commonly, linear regression refers to a model in which the conditional mean of y given the value of X is an affine function of X.

Example: Consider a situation where a small ball is being tossed up in the air and the measure its heights of ascent h at various moments in time t. ignoring the drag, the relationship can be modeled as

$$H = \beta t + \alpha t^2 + \varepsilon$$

Where
β = the initial velocity of the ball,
α is proportional to the standard gravity, and
ε is due to measurement errors.

Application of linear regression

- Trend line -the long-term movement in time series data after other components have been accounted for.
- Finance
- Economics
- Environmental science

F. Encrypting image: Encryption is a process of converting data in one form to the other such that the input data which was in an easy understandable form is converted to less understandable format after encryption.

G. Constructing Steganoimage: The encrypted image cannot be send as such to the receiver since it may be hacked by the intruders so the encrypted image is next put into a process of steganography. The method followed for embedding encrypted image in the cover image is named as Quad Conceal steganography. The following are the steps for constructing stegano image.

Step 1: The encrypted image is now converted into binary form such that each pixel value contains 8 bits of value.

Step 2: The cover image is now divided into four equal parts. Such that each sub divided part is of the size of secret image or the encrypted image.

Step 3: Cover image is also converted into binary values each comprising of 8 bits.

Step 4: The encrypted image's binary values are now divided into 4 groups each containing two bits.

Step 5: The first two bits of MSB of the first pixel are replaced as last two bits in the first cover image group's first pixel. Similarly the second two MSB of the first pixel are replaced as last two bits in the second cover image group's first pixel.

Step 6: Repeat step 5 for all pixels.

Step 7: Finally convert the binary values into integers and thus it forms the stegano image.

H. Transmitting data: The stegano image after all process is transmitted to the receiver.

I. Reconstruction of stegano image: The stegano image received by the receiver is to be reconstructed to extract the information hidden. The reverse operation of the construction process is performed to reconstruct the image. After performing all steps the encrypted image will be obtained.

J. Decrypting image: The encrypted image obtained is now applied with the steps of encryption in reverse manner. This process will yield the input secret image. The key character used in decryption process is also the same as in encryption.

The proposed methodology is represented diagrammatically for ANN based multi resolution Rubik's magic cube method as given below.

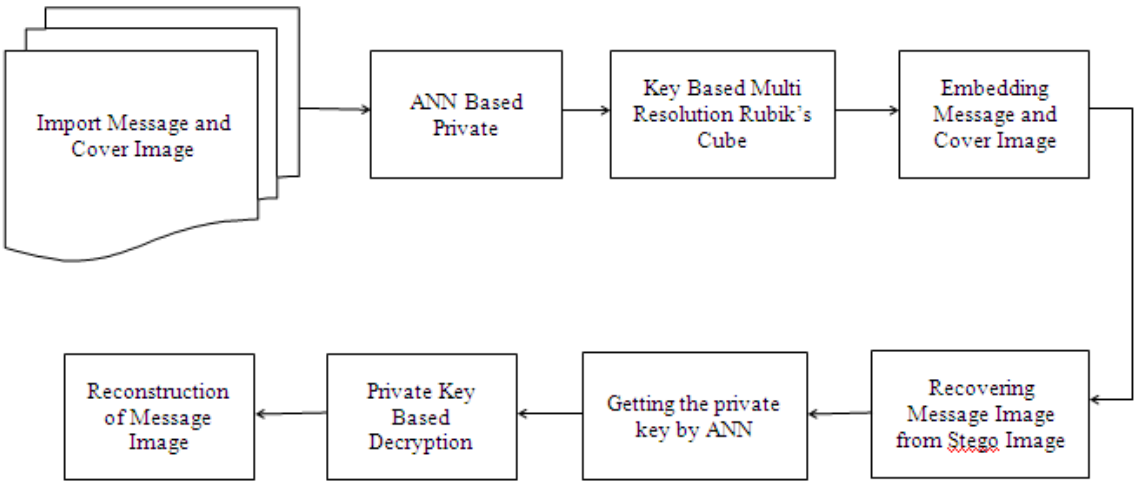

Figure-3. An overview of the proposed methodology.

ALGORITHM FOR ANN BASED RUBIK'S MAGIC CUBE METHOD

Step 1: Consider a square matrix of image. Perform the sum of elements in all individual rows. If the sum of first row elements is even, perform a right circular shift of that particular row and perform left circular shift if it is odd. Repeat this for all rows.

Step 2: Now perform column wise sum of all elements. If the sum of first column elements is even, perform a down circular shift of that particular row and perform up circular shift if it is odd. Repeat this for all columns.

Step 3: Convert the finally obtained image matrix data into binary form with each pixel converted into 8 bits. Now perform an XOR operation between binary value of one single key letter say 'k' represented in 8 bits and every element in the binary value matrix.

Step 4: After performing XOR operation, the matrix is again converted into integers form. And that form the encrypted image. Generate randomly two vectors KR and KC of length M and N, respectively. Element (i) and KC (j) each take a random value of the set $\mathcal{A}$= {0, 1, 2, 2 α −1}. Note that both KR and KC must not have constant values.

Step 5: Determine the number of iterations, ITER max, and initialize the counter ITER at 0.

Step 6: Increment the counter by one: ITER=ITER+1.

Step 7: For each row i of image I,

Compute the sum of all elements in the row, this sum is denoted by (i),

(i)= N. j=1 lo $(i,)$, =1, 2..,

(b) Compute modulo 2 of $\alpha(i)$, denoted by $M\alpha(i)$,

(c) Row i is left, or right, circular-shifted by KR (i) positions (image pixels are moved KR (i) positions to the left or right direction, and the first pixel moves in last pixel.), according to the following:

If (i) =0⟶right circular shift Else⟶ left circular shift

Step 8: For each column j of image,

(a) Compute the sum of all elements in the column, this sum is denoted by (j),

$(j)= M \cdot i=1$ lo $(i,)$, =1, 2… N,

(b) compute modulo 2 of $\beta(j)$, denoted by $M\beta(j)$.

(c) Column$j$ is down, or up, circular-shifted by KC (i) positions, according to the following:

If (j) =0⟶upcircularshiftelse⟶downcircularshift. (7)

Steps 7 and 8 above will create a scrambled image, denoted by I SCR.

Step 9: Using vector, the bitwise XOR operator is applied to each row of scrambled image I SCR using the following expressions:

IENC1 $(2i-1, j)$ =I SCR $(2i-1,) \oplus KC$ I (j),

ENC1 $(2i, j)$ = I SCR .K $(2i,) \oplus$rot180 $C.(j)$ (8),

Where$\oplus$ and rot180 (KC) represent the bitwise XOR operator and the flipping of vector KC from left to right, respectively.

Step 10: Using vector, the bitwise XOR operator is applied to each column of image $I1$ using the following formulas:

IENC $(i, 2j-1)$ =I1 $(i, 2j-1) \oplus KR$I (j),

ENC $(i, 2j)$ =I1.K $(i, 2j) \oplus$rot180 RI (j), (9),

With rot180 (KR) indicating the left to right flip of vector KR.

Step 11: If ITER=ITER max, then encrypted image IENC is created and encryption process is done; otherwise, the algorithm branches to step 3. The encrypted image is now converted into binary form such that each pixel value contains 8 bits of value.

Step 12: The cover image is now divided into four equal parts. Such that each sub divided part is of the size of secret image or the encrypted image. Cover image is also converted into binary values each comprising of 8 bits.

Step 13: The encrypted image's binary values are now divided into 4 groups each containing two bits. The first two bits of MSB of the first pixel are replaced as last two bits in the first cover image group's first pixel. Similarly the second two MSB of the first pixel are replaced as last two bits in the second cover image group's first pixel.

Step 14: Repeat step 3 for all pixels. Finally convert the binary values into integers and thus it forms the stegano image.

Vectors and the max iteration number ITER max are considered as secret keys in the proposed encryption algorithm. However, to obtain a fast encryption algorithm it is preferable to set ITER max =1 (single iteration). Conversely, if ITER MAX >1, then the algorithm is more secure because the key space is larger than for ITER MAX =1. Nevertheless, in the simulations presented in Step 6, the number of iterations ITER max was set to one.

4. RESULTS AND DISCUSSIONS

The algorithm is implemented in Pentium IV using MAT Lab R 2013.The Experimental Result shows that the proposed methodology performance is better than the multistage image encryption using Rubik's cube for secured image transmission. Here large data set was substituted and verified (Shown in the Table). The PSNR value is calculated for the image after the decryption at the receiver end as well as for the original image. The experimental result is given in the below table.

Table-1. Results for ANN based Rubik's cube method.

S.No	Image No.	PSNR	NPCR-R plane	NPCR- G plane	NPCR- B plane	Time consumed for (Secs)	
						Encryption	Decryption
1	Image1	Infinity	98.43	98.628	99.6723	4.32	4.28
2	Image2	Infinity	98.64	99.25	98.26	4.86	4.69
3	Image3	Infinity	99.654	99.345	99.543	5.02	4.82

Figure-4. Message image.

Figure-4(a). Cover image.

Figure-4(b). Stegoimage.

Figure-4(c). Reconstructed image.

Figure-4(d). Recovered image.

Figure-5. Message image.

Figure-5(a). Cover image.

Figure-5(b). Ann key based encryption.

Figure-5(c). Stegoimage.

Figure-5(d). Reconstructed image.

Figure-5(e). Recovered image.

Figure-6(a). Message image.

Figure-6(b). Cover image.

Figure-6(c). Ann key based encryption.

Figure-6(d). Stegoimage.

Figure-6(e). Reconstructed image.

Figure-6(f). Recovered image.

5. CONCLUSION

In this paper an attempt has been made to propose a better image hiding algorithm for secured data communication. Steganography is the data hiding technique which comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to obscure the very existence of the embedded image. Here the confidential image is embedded into an image file in such a manner that the degradation in quality of the carrier image is not noticeable. The experimental results show that the time taken to embed the data into the image is high and suitable for digital data transmission through internet and other communication systems.

REFERENCES

[1] ArunA.S and George M. Joseph. 2013. High Security Cryptographic Technique using Steganography and Chaotic Image Encryption.In Proc. of Journal of Computer Engineering (IOSRJCE). 2: 49-54.

[2] Moerland T. Steganography and Steganalysis. Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf.

[3] L. Yu, Y. Zhao, R.Ni and T.Li. 2012. Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm.In Proc. of EURASIP Journal on Advances in Signal Processing. 10: 1-6.

[4] MehrotraKishan, Chilukuri K. Mohan and Sanjay Ranka. 1997. Elements of Artificial Neural Networks. The MIT Press, Boston.

[5] SumitGoyal and Gyandera Kumar Goyal, August. 2011. Cascade and Feed forward Back propagation Artificial Neural Network Models for Prediction of Sensory Quality of Instant Coffee Flavored Sterilized Drink. Canadian Journal on Artificial Intelligence, Machine Learning and Pattern Recognition. 2(6).