Neural Comput & Applic (2015) 26:111–116
DOI 10.1007/s00521-014-1702-1

ORIGINAL ARTICLE

Artificial neural network for steganography

Sabah Husien · Haitham Badi

Received: 13 April 2014 / Accepted: 14 August 2014 / Published online: 28 August 2014

Abstract The digital information revolution has brought about changes in our society and our lives. The many advantages of digital information have also generated new challenges and new opportunities for innovation. The strength of the information hiding science is due to the nonexistence of standard algorithms to be used in hiding secret message. Also, there is randomness in hiding method such as combining several media (covers) with different methods to pass secret message. Information hiding represents a class of process used to embed data into various forms of media such as image, audio, or text. The proposed text in image cryptography and steganography system (TICSS) is an approach used to embed text into gray image (BMP). TICSS is easily applied by any end user.

Keywords Human–computer interaction · Artificial neural network · System identification · Neuro-identifier · Cryptanalysis

1 Introduction

Information hiding is the art of hiding message inside other message. In other words, information hiding studies the way that make communication invisible by hiding secret in innocuous message. This part of information hiding called steganography. Steganographic methods usually hide messages in others, harmless looking data in such that, third person can not detect or even prove this processes [1]. Another technique for hiding information is digital watermarking, digital watermarking addresses issues related to intellectual property and copyright protection. Digital watermarking can be thought of as commercial applications of steganography and may be used to trace, identify, and locate digital media across networks. Digital watermarks are attributes of the carrier, as a watermark typically includes information about the carrier or the owner [1].

1.1 Artificial neural networks (ANN)

An artificial neural network (ANN) is an information processing paradigm that is inspired by biological nervous systems, such as the way the brain processes information. The key element of this paradigm is the novel structure of the information processing system. ANN is composed of a large number of highly interconnected processing elements (neurons) that work in unison to solve specific problems. Similar to the human brain, ANNs learn by example [2]. A neural network consists of interconnected processing units that operate in parallel. Each unit receives inputs from other units. The unit then obtains the sum of these inputs and calculates the output, which is then sent to the other units it is connected to. The learning or the knowledge acquisition results from the modification of the strength of the connection (weight) between the interconnected units system. Thus, an ANN has been a lively field of research [3–8].

1.2 Supervised learning

Supervised learning, which is a commonly used training method, is based on a system aiming to predict outcomes

S. Husien (✉)
Al Yarmouk University College, Baghdad, Iraq
e-mail: prof.sabah@hotmail.com

H. Badi
University of Malaya, Kuala Lumpur, Malaysia

for known examples. Supervised learning compares its predictions to the target answer and learns from its mistakes. The data start as inputs to the input layer neurons. The neurons pass the inputs along the next nodes. Weights or connections are applied as inputs and are passed along. When the inputs reach the next node, the weights are summed and are either intensified or weakened. This process continues until the data reach the output layer where the model predicts an outcome. In a supervised learning system, the predicted output is compared with the actual output for that case. If the predicted output is equal to the actual output, then no change is made to the weights in the system. However, if the predicted output is higher or lower than the actual outcome in the data, the error is propagated back through the system and the weights are adjusted accordingly. This backward feeding of the error through the network is called back-propagation. Both the multilayer perceptron and the radial basis function are supervised learning techniques. The multi-layer perceptron uses back-propagation, whereas the radial basis function uses a feed-forward approach that trains on a single pass of data [9].

1.3 Advantages of neural computing

Neural networks offer analysts a variety of benefits [9]. (1) Artificial neural networks are a powerful technique for harnessing the information in the data and for making generalizations about this information. Neural networks learn to recognize patterns in the data set [10]. (2) The system is developed through learning rather than through programming. Programming is much more time consuming for the analyst and requires the analyst to specify the exact behavior of the model. Neural networks teach themselves the patterns in the data, freeing the analyst for more interesting work [11]. (3) Neural networks are flexible in changing environments. Rule-based systems or programmed systems are limited to the situation for which they were designed; when conditions change, the rules are no longer valid. Although neural networks may take some time to learn a sudden drastic change, they excel at adapting to constantly changing information [12]. (4) Neural networks can build informative models where more conventional approaches fail. Neural networks can handle very complex interactions and can thus easily model data that are too difficult to model by using traditional approaches, such as inferential statistics or programming logic [11]. Neural networks perform at least as well as classical statistical modeling and outperform the latter on most problems. Neural networks build models that are more reflective of the structure of the data in significantly less time [12].

1.4 Data security

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure and modification [13]. Data in computer systems are in danger from many threats including indiscriminate searching, leakage, inference, and accidental destruction as showing in Fig. 1 [14]. There are two principal objectives known as secrecy (or privacy), which is to prevent the unauthorized disclosure of data, while the other is authenticity (or integrity), to prevent the unauthorized modification of data. Information transmitted over electronic lines is vulnerable to passive wiretapping, which threatens secrecy, and to active wiretapping, which threatens authenticity [13]. Passive wiretapping (eavesdropping) refers to the interception of message contents usually without detection. Although it is normally used to disclose message contents, in computer networks, it can also be used to monitor traffic flow through the network to determine who is communicating with whom [13]. Active wiretapping (tampering) refers to deliberate modifications made to the message stream. This can be for the purpose of making arbitrary changes to a message, or replacing data in message with replays of data from earlier message. It can be for the purpose of injecting false messages, injecting relays of previous message, or deleting message [13].

1.5 Information hiding

Information hiding represents a class of process used to embed data into various forms of media such as image, audio, or text. There are two types of information hiding: The first one is steganography and the second is digital watermarking. Steganography serves to hide secret messages in other messages, such that the secret's very existence is concealed. Generally, the sender writes an innocuous message and then conceals a secret message on the same piece of paper [15]. Steganography has its place in security. It is not intended to replace cryptography but to supplement it. Hiding message with steganography reduces the chance of a message being detected [15]. Digital watermarking, some of the objectives of using this techniques are confirmation of property, follow up of unauthorized copies, validation of identification and verification of integrity, labeling, usage control and protection of contents [16].

There are three main types of Steganography as illustrated in Fig. 2.

Pure Steganography: We call a steganographic system which does not require the prior exchange of some secret information (like a stego key) pure Steganography. Formally, the embedding process can be described as a mapping E: CxM, where C is the set of possible covers and M

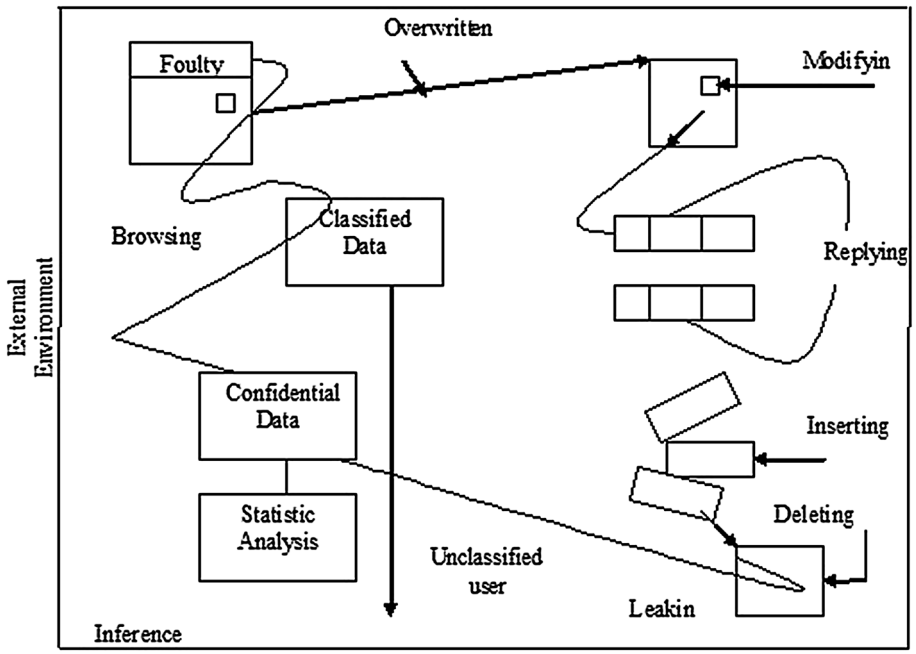

Fig. 1 Threats to data stored in computer system

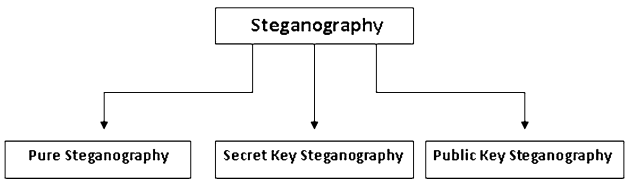

Fig. 2 Steganography types

the set of possible messages. Secret key steganography: A secret key steganography system is similar to a symmetric cipher: The sender chooses cover C and embeds the secret message into C using a secret Key K. If the key used in the embedding process is known to the receiver, he can reverse the process and extract the secret message. Anyone who does not known the secret key should not be able to obtain evidence of the encoded information. Again, the cover C and the stego object can be perceptually similar. Public key steganography: Publickey steganography system requires the use of two keys—one is private and the other one is public key; the public key is strode in a public database, whereas the public key is used in the embedding process, the secret key is used to reconstruct the secret message [15]. In public key cryptography, it is not necessary for two people to share a secret key to establish a secure channel. One only needs to know the other's public key. This suggests a possible approach to steganography in which a secret key does not have to be agreed upon by sender and recipient prior to imprisonment. Some information must still be known a priori one prisoner must know the other's public key but from a practical perspective this is a much more reasonable requirement [17].

2 Background studies

Fridrich et al. [18, 19] Introduced the dual statistics steganalytic method for detection of LSB embedding in uncompressed formats. For high quality images taken with a digital camera or a scanner, the dual statistics steganalysis indicates that the safe bit-rate is <0.005 bits per sample, providing a surprisingly stringent upper bound on steganographic capacity of simple LSB embedding [20]. The system applied on color image and used LSB method the system depend on the ASCII value of character and compares it with value of palette of picture then if equally, the position of value palette substitutes in other place [21]. This system uses two methods: butter fly technique and chess technique to embed a text in image using format (BMP, GIF and JPEG) [22]. In this work, he tried to design an efficient system to scan and test suspicious images to find out if it contains a secret message or not. The systems try to extract the secret message (the secret message may be text or image) from the suspicious image (if it is possible) and make changes on it. When failed to extract the secret message or to prevent suspicion image for pass a secret message, the system has the ability to destroy the secret messages.

3 Methodology

3.1 Terminology

Cryptography is the science of designing cipher systems and cryptanalysis is the name given to the process of

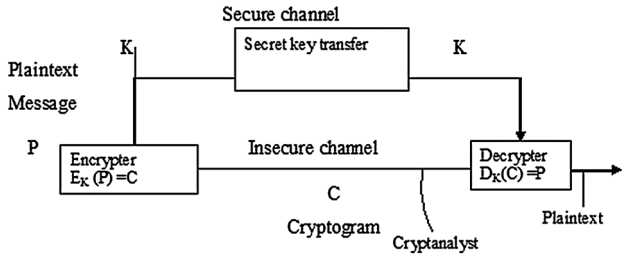

Fig. 3 Cipher system

deducing the plaintext from the ciphertext without knowing the secret key. Cryptology includes both cryptography and cryptanalysis. A cipher is a secret method of writing. The idea of cipher system as shown in Fig. 3. Is to disguise confidential information in such away that its meaning is unintelligible to unauthorized person. The information to be concealed is called the plaintext P (or just the message) and the operation of the disguising it is known an enciphering or encryption EK(P). The enciphered message is called the ciphertext or cryptogram C. The person who enciphers the message is known as the encipherer, while the person to whom he sends the cryptogram is called the recipient or receiver. The set of rules operation of this algorithm will depend on the secret key K chosen by the encipherer. The inputs to the algorithm are hence the secret key and the message. It is absolutely crucial that the recipient knows the key and that this knowledge should enable him to determine the plaintext uniquely the process of applying a key to translate both from the ciphertext to the plaintext is known as deciphering or decryption DK(C). Any person who intercepts the cryptogram in order to try to break the system is called cryptanalyst [23].

3.2 Nuero-identifier

The procedure begins with the choice of neural model which is defined by its architecture and an associated learning algorithm. This choice can be made through trial and error. Once the neural model is, and system input-output data are available, learning can begin. Different structures are trained and compared using learning set and simulation set of data, and a criterion (error goal) [24, 25]. The optimal structure, then, is the one having the fewest units (neurons) for which the criterion is met. Neuro-identifiers (NID) are basically multi-layer feed-forward (MLFF). Artificial neural networks with an input layer (buffer layer), a single or multiple nonlinear hidden layer with biases, and a linear/or nonlinear output layer [26, 27]. The results of research have shown that linear identifiers are not capable of identifying nonlinear systems. Hybrid identifiers can identify simple nonlinear system, but not complex ones [27–29]. Figure 4 Illustrates the structure of

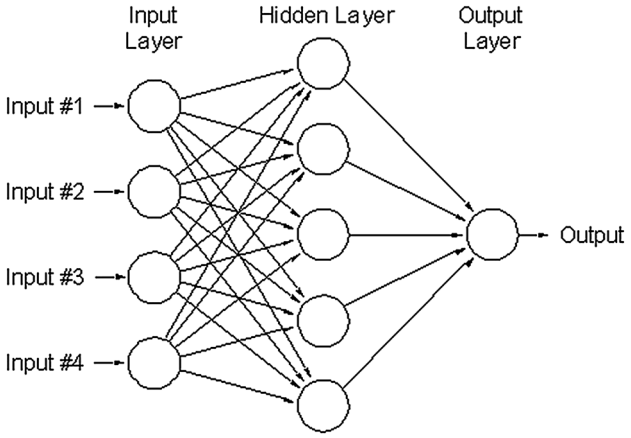

Fig. 4 Multi-layer feed-forward neural identifier architecture

the multi-layer feed-forward neural network identifier NID, with two nonlinear hidden layers, the size of the neural network is crucial in designing the whole structure. There is no mathematical formulation to calculate the optimal size of such networks. However, with many free units the NID will learn faster, avoid local minima, and exhibit a better generalization performance [30, 31]. The essential constraint on increasing the size of hidden layers is the limitation of the hardware architecture used in the experimental work.

3.3 System theoretic approaches to stream cipher design

As mentioned earlier, stream cipher design is a lot like block cipher design. It involves more mathematical theory, but in the end, a cryptographer proposes a design and then tries to analyze it. According to Rueppel [32, 33], there are four different approaches to the construction of stream ciphers: (1) system theoretic approach— try to make sure that each design creates a difficult and unknown problem for the cryptanalyst, using a set of fundamental design principles and criteria; (2) Information theoretic approach —try to keep the cryptanalyst in the dark about plaintext. No matter how much work the cryptanalyst invests, he will never get a unique solution; (3) Complexity theoretic approach—try to base the cryptosystem on, or make it equivalent to, some known and difficult problem such as factoring or taking discrete logarithms; and (4) Randomized approach— try to generate an unmanageably large problem by factoring the cryptanalyst to examine lots of useless data in his attempts at cryptanalysis. The system theoretic approach was used in all the known stream ciphers, it produces most of the stream ciphers that are practical enough to be used in the real world. A cryptographer designs keystream generators that have testable security properties (period, distribution of bit patterns,

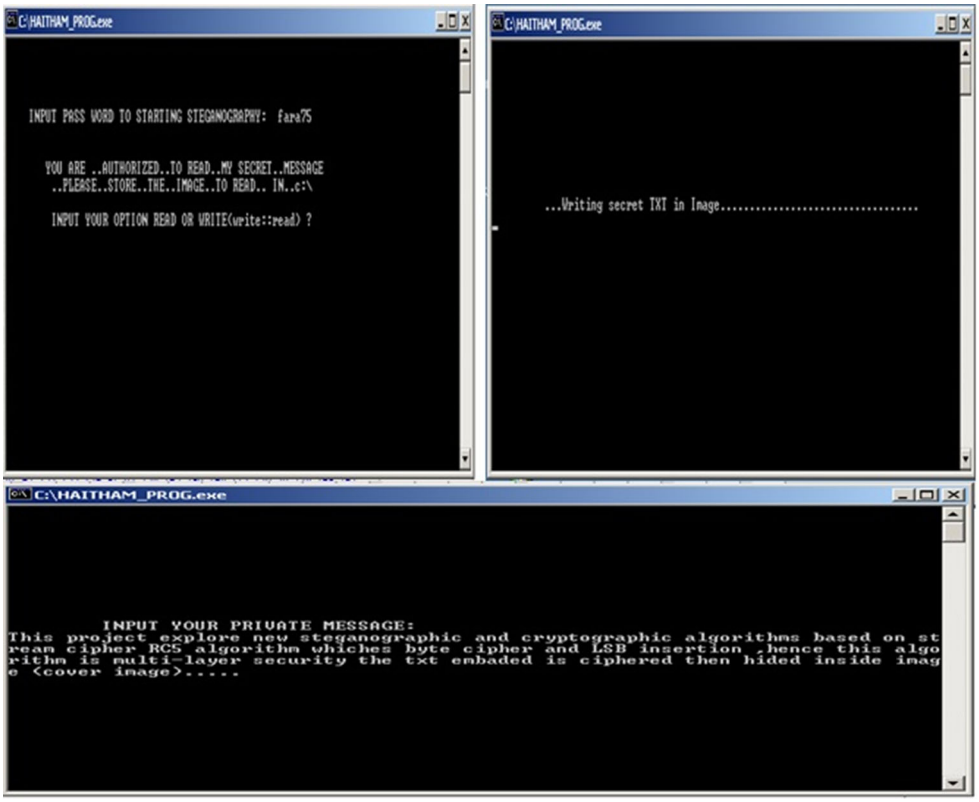

Fig. 5 System implementation

linear complexity, and so on) and not ciphers based on mathematical theory. The cryptographer also studies various cryptanalytic techniques against these generators and makes sure the generators are immune to these attacks. The design criteria for stream ciphers that were discussed by Rueppel [33] are as follows: (1) Long period, no repetition; (2) Linear complexity criteria, large linear complexity, linear complexity profile, local linear complexity; (3) Statistical criteria such as ideal k-tuple distributions; (4) Confusion-every key stream bit must be a complex transformation of all or most of the key bits; (5) Diffusion redundancies in substructures must be dissipated into large-ranges statistics; and (6) Nonlinearity criteria for Boolean functions like *m*th-order correlation immunity distance to linear functions, avalanche criterion.

4 Experiments and results

The simulation package for our system starts asking the user to select one from two phases: The first phase is writing in which the secret image is fed to the hiding software and the hiding process is begin transferred to the second stage. The second stage of our proposed package starts by asking the user to select one of two actions: The first action is write, which is stands for writing secrete message into the cover image, whereas the second action is to read the secrete message from the cover image. The third stage of the proposed algorithm includes the input of the secret massage we want to embed inside the cover image as shown in Fig. 5.

5 Conclusions

The Levenberg–Marquardt (LM) algorithm from neural network is used to train the neuro-identifier which gives good approximation capabilities, faster convergence, and more stable performance surface. It enables the user to provide the system with both text and cover, and to obtain a resulting image that contains the hidden text inside. Steganography is not intended to replace cryptography but rather to supplement it. If a message is encrypted and hidden with a steganographic method, it provides an additional layer of protection and reduces the chance of the hidden message being detected. TICSS can be defined as a secret key steganography since it shares a secret key between sender and receiver, in this system, there is no need for the knowledge of original cover in the extraction process. The amount of the information embedded in the other media depends on the statistical properties of the cover media, where this amount is small the noise in the media is not perceptible. From the implementation, we conclude that the TICSS is

very rapid in performing extraction process and the size of the embedded text does not affected the speed of the system very much.

References

1. Johnson NF, Duric ZJ (2001) Information hiding steganography and watermarking attack and countermeasure. Kluwer Academic Publishers, Norwell, MA
2. Stergiou C, Siganos D (1996) Neural networks. http://www.doc.ic.ac.uk/∼nd/surprise_96/journal/vol4/cs11/report.html. Retrieved Mar 2008
3. Hasan H, Abdul Kareem S (2012) Static hand gesture recognition using neural networks. Artif Intell Rev
4. Hasan H, Abdul Kareem S (2013) Fingerprint image enhancement and recognition algorithms: a survey. Neural Comput Appl 23:606–1608
5. Hasan H, Abdul Kareem S (2012) Static hand gesture recognition using neural networks. Artif Intell Rev. doi:10.1007/s10462-011-9303-1
6. Hasan H, Abdul Kareem S (2013) Human–computer interaction using vision based hand gesture recognition systems:a survey. Neural Comput Appl. doi:10.1007/s00521013-1481-0
7. Sabah H, Hussien H (2014) Hand posture and gesture recognition technology. Neural Comput Appl. doi:10.1007/s00521-014-1574-4
8. Badi H, Hussien S, Abdul Kareem S (2014) Feature extraction and ML techniques for static gesture recognition. Neural Comput Appl. doi:10.1007/s00521-013-1540-6
9. Symonidis K (2000) Hand gesture recognition using neural networks. Master thesis, School of electronic and electrical engineering
10. Haykin S (1994) Neural networks a comprehensive foundation. Macmillan College Publishing Company, New York
11. Moghadassi A, Parvizian F, Hosseini S (2009) A new approach based on artificial neural networks for prediction of high pressure vapor-liquid equilibrium. Aust J Basic Appl Sci 3(3):1851–1862
12. Din A (2002) Optimization and forecasting with financial time series. Paper presented at the note from seminar at CERN
13. Dorothy E, Denning R (1983) Cryptography and data security. Addison Wesley Publishing Company Inc., Boston, MA
14. Lane V (1988) Security of computer based information system. Macmillan Education LTD, New York, NY
15. Johnson (2001) Information hiding steganography and watermarking attack and countermeasures. Kluwer Academic Publishers
16. Benjamin B, Santiago G, Victor B (2001) Steganographic watermarking for documents. In: Proceeding on the 34th Hawaii international conference on system science
17. Craver S (1998) On public-key steganography in the presence of an active warden information hiding, second international workshop proceeding, vol 1525, pp 355–368
18. Fridrich J, Goljan M, Du R (2001) Detecting LSB steganography in color and grayscale image, magazine of IEEE multimedia special issue on security, October–November issue, pp 22–28
19. Fridrich J, Goljan M, Du R (2001) Reliable detection of LSB steganography in grayscale and color images. In: Proceedings of the ACM, special session on multimedia security and watermarking. Ottawa, Canada, pp 27–30
20. Uruba I (2001) Hiding text in image. M.Sc. Thesis, University of technology, Computer Science Department
21. Mohammed S (2001) Text file hiding techniques with implementation. M.Sc. Thesis, National Computer Center
22. Al-hamami M (2002) Information hiding attack in Image. M.Sc.thesis, Iraqi commission for computer and informatics, Informatics Institute for Postgraduate Studies
23. Petitcolas, Fabien A, Ross J (1998) Attack on copyright marking systems information hiding, second international workshop proceeding, vol 1525, pp 218–238
24. Thomas B (2008) Quantitative security of block ciphers designs and cryptanalysis tools. PhD Ecole Polytechnique Federale De Lausame, Suisse
25. Zehnran J, Yanhong Z (2006) Using gene neural network to D target identification. J Integr Bioinform 1(2):26–28
26. Sarle S (1999) Artificial neural networks and their biological motivation internet explorer. Artif Intell Worlf Wide Navig. http://www.csa.ru
27. Whitefield D, Martin H (1979) Privacy and authentication an introduction to cryptography. Comput J IEEE 67(3):397–427
28. Khaled A, Waiel F, Mohamed A, Alaa A (2010) Attack and construction of simulator for some of cipher system using neuro-identifier. Int Arab J Inf Technol 7(4):365–372
29. Tanomaru J (2002) Comparative study of two neuro network approaches for nonlinear identification. In: Proceeding of international symposium on speech image processing and neural networks. Hong Kong, pp 487–490
30. Josef P, Jennifer S (1988) Cryptography an introduction to computer security. Prentice Hall, Upper Saddle River
31. Zabikowski R, Dzielinski A (1995) Neural approximation a control perspective. In: Proceeding of neural network engineering and dynamic control systems, advances in industrial control. Berlin, pp 1–25
32. Ruppel RA (1992) Security models and notions for stream cipher, cryptography and coding II. Mitchell press, Burnaby, BC
33. Ruppel RA (1992) Stream ciphers contemporary cryptology, the science of information integrity, Simmons, j. IEEE Press