Conference Info
International Conference on Latest Concepts in Science, Technology, Management and Humanities (ICLCSTMH-2017)
(NITTTR) National Institute of Technical Teachers Training & Research, Chandigarh, India (MHRD, Govt. of India)
on 2nd April 2017 ISBN: 978-81-933746-4-1

Use of Hybrid Fuzzy Neural Network for Advanced Steganography

Amit Aher, Akshay Bakliwal, Pandurang Sadgir, Suraj Zankar, V.S. Tidake
Department of Computer Engineering
NDMVPS's KBTCOE, Nashik, Maharashtra

ABSTRACT
In today's world steganography is very important due to the confidential communication between computer users over theinternet.Steganographyisknownastheapplicationofnon-visibletransmissionwhich is accomplishedbycloakingthe presence of any communication. Generally, data embedding is attained in various multimedia formats like image, text, audio,and is heavily used in army for transmitting sensitive information, copyright, attestation and various other government sectors and general purpose. In the steganography technique, covert communication is done by embedding some information inside the cover media a.k.a. carrier and produce a stego-image i.e. output image that consists of concealed secret information. The analysis of various steganographictechniquesandfurtherprocessingofthestego-imageisdoneusingtheHybridFuzzyNeuralNetwork is used in the system. The pixels where secret message is to be embedded is selected by using the AES encryption algorithm.Thehybridfuzzyneuralnetworkisusedtohandletheresultantstego-imagequalitywhichcanbedegraded due to the embedding of secret message. This method can achieve better embedding capacity with excellent stego- image quality and high security of secret message confidentiality. Also, analysis of Steganography, its main types, their classification and applications arereviewed.

Keywords
Steganography, Secret communication, digital image, Artificial Intelligence, Fuzzy Neural Networks, Stego-image.

1. INTRODUCTION

Steganography is a useful methodology for keeping the information hidden, it is mainly used to conceal the presence of any secret transmission and to keep the data secret from any third party i.e. to intelligently securing the data transfer. A message is implanted into a "carrier media" using a steganographic algorithm. In the digital world, different types of digital media can be used as the transmitter ("carrier medium") such as image, audio, video, even various internet protocols and the message like image or text ("Secret data"). In the modern era "Steganography" word normally refers to information which is been covered into a digital image, audio or video file. In general, the human eyes are not capable to identify the files that stores some hidden information internally. In today's digital world the digital communication plays the major role where the high-speed internet connectivity is available. As compared to Analog media, Digital media offers some discrete advantages such as good quality, smooth editing, great accuracy in copying as well as compression etc. [6]. But this type of improvement in the area of data communication has elevated the concern of data being snooped by any intruderwhile transmitting it from the sender to the receiver. Hence, Data Security is becoming a most important component of digital data communication. Hence, to obtain information security, Steganography performs an essential task for maintaining the integrated data security while sending it to nominated receiver. In this method no-one rather than the authorized sender and designated recipient, recognizes there is a hidden message present in communication. This paper is a good review of the steganography techniques appeared in the research of various digital information security domains present in today's digitalized world.

2. RELATEDWORK

2.1 Concept ofSteganography

Digital communication has become a necessary part in today's world as there are lots of applications which uses the internet. Therefore, the communication made must be private. Security techniques like"cryptography" are used widelyto transmit the information privately. Steganography is anadvanced way of implementingprotected data transmission. "Steganography"is named after a Greek word "steganos" which means hidden or secret, and "graphy" meaning writing - literally mean as "covered writing" [1]. Usually, Steganography is known as "invisible" communication. Steganography is the science and art of hidden

communication, practiced through concealing secret information into a carrier object. Since from ancient times the Steganography technique has been used across the world, widely it is famous during World War times. Steganography techniques can be characterized into two types based on the mode of intervention by the superintendent user who has been designated to recognize & eliminate secret communication – these are called "Active" and "Passive" modes of Steganography. In Active mode of Steganography, the superintendent user tries to change the communication with the possiblesecret information carefully, to extract the secret information. On the other hand, in passive mode, the superintendent user simply parses the trasnsmission going on and figures out whether it likelyhave somesecret information. For any suspected message containing hidden communication, he would take notes of the revealed secret transmission, convey this to the higher authority and permits the message through to the intended receiver without blocking it [7].

2.2 Definitions in DigitalMedia

Computerized digital media are encoded within a machine i.e. a computer system which can be easily created, viewed, shared, changed and stored on computer machines. Steganography can be used for almost all digital file formats, however the formats that are more suitable are those with a higher degree of redundancy. Redundancy can be interpreted as the bits of an object which contributes to the efficiency which is necessary for the object's usability and presentation. Image and audio files specifically used with this concern, while research has also proved that network protocols can also be used for secret message tranmission.

Audio

A digital audio is seen by a computer as a sequence of 0's and 1's which is also called as a bit stream. An analog signal is continuously sampled at a specific rate to produce a discrete audio signal. In this digital era, to store audio, PCM (Pulse Code Modulation) is the most widely used sampling mechanism. "Nyquist theorem" is used to sample the analog audioand also to preserve the respective samples in a sequential binary form

Image

Digital Images are nothing but the snapshots of the current screen or scanned documents such as photographs, papers, printed writings, and any artwork. The digital image is a collectionof picture elements (pixels) made up of RGB values. Each pixel of an image hold a specific value represented in binary form (0s and 1s) which represents colors such as black, white or shades of grey. The binary digits ("bits") for each pixel are stored sequentially by a computer and usuallycompressed to a mathematical representation format. The bits are analyzed and accordingly the computer generates an analog version for display.

Text

The plain text is made up of simple sequence of characters according to standards mentioned by Unicode. Plain text is unrestricted, regulated, and completely readable. Whereas, styled text (rich text) is a text representation consisting of plain text formed with information like language identifier, font size, font color, hyperlinks, etc. Rich text such as RTF, HTML, XML, and TEX used in real-time are all based on plain text.

Video

Highly correlated signals are known as a video, this correlation has occurred from two sources, first is the spatial correlation which is the outcome of correlation between neighbouring pixelsin each frame of the video sequence. The other one is the temporal correlation which is shown by slowing the time varying nature of the video signals. [3]

2.3 Different kinds of Steganography in DigitalMedia

Steganography can be classified into 4 subtypes based on the use of various kinds of computerized digital media as a carrier:

(a) Image Steganography - done on image files
(b) Audio Steganography - done on audio files
(c) Video Steganography - done on video files
(d) Network Steganography - done on network protocols

(a) ImageSteganography

The largest well-familiar fashion of steganography involves cloaking messages within digital images. This can be accomplished by manipulating the low order bits of an image, as a result the modification in the image can be hardly noticed, but a difference in the modified image with the original image denotes an arrangement resembling in a hidden message. This kind of steganography is mostly performed on bitmap images because of their simplicity in representingthe data as the image itself remains completely unaltered visually by simply flipping the low order bit of an image. JPEG images are also used in this type of steganography using software like JSteg. JPEG images are difficult to modify because of the layered structure & embedding of data in this structure is very complex as compared to thesimple data format for bitmap images.

(b) AudioSteganography

Audio Steganography deals with embedding secret messages into a digital audio file. The embedding of secret messages in an audio format is rather more complex as compared to embedding done into text, image. Audio Steganography is supported to WAV, MP3 audio files. The process of Audio Steganography makes use of the characteristics which are very similar to that of the Human Auditory System (HAS). A critical band analysis on the inner ear is done where a frequency-to-location transformation is performed within a basilar membrane which is necessary for auditory perception.

Performance Measure

This measure is used for image distortion which occurs as a result of embedding.This can be represented by peak-signal-to-noise ratio (PSNR). Higher the PSNR, better is the image quality. It is defined as:

$$PSNR = 10\log(\frac{{C_{max}}^2}{MSE})$$

here MSE is the mean square error, shown as:

$$MSE = \frac{I}{AB}\sum_{x=1}^{A}\sum_{y=1}^{B}\left(S_{xy} - C_{xy}\right)^2$$

(c) Video Steganography

Video steganography in recent times has gained lot of popularity among researchers. As a video can be thought of audio & collection of frames/images, it provides a very convenient way for embedding data. In Steganography using video files as a shipping medium is further suitable as compared to other techniques.Using video steganography file/information in any format can be embedded into the digital audio file. AVI, MPEG & also some other video file formats are supported.[2].

Performance Measure

Quality of any steganography technique is described mainly by two attributes, one is the imperceptibility which says that the embedded data must not be visible to the third party/observer and any statistical analysis done by the computer. And other is capacity stating the amount of data that can be embedded in files.

The original image or video is compared to its stego-counterpart to find out their visual differences, if there are any, are determined. This indicates the perceptual imperceptibility of the embedded data to the naked eye.

The Mean squared Error (MSE), Peak Signal to Noise Ratio (PSNR) and Image Fidelity (IF) between the "Stego- frame" (frame with hidden data) and its corresponding cover frame (original frame) are compared. The quantities are given as below,

$$MSR = \frac{1}{H * W}\sum_{x=1}^{H}\left(P(x,y) - S(x,y)\right)^2$$

Here, MSE represents the Mean Square Error, H denotes the Height, W shows the Width and P(x,y) serves as the original frame and S(x,y) as the corresponding stego-frame. PSNR stands for Peak-Signal-To-Noise-Ratio, where L representsthe peak signal level.When working with a grey-scale image its value is taken as 255 tone color.

(d) NetworkSteganography

The loopholes in the normal data transmissions of users are used for sending secret data in Network Steganography. It can be seen as a risk to network security, as they may be used forleaking confidential information.

Network steganography can be categorized in three groups:

- Methods which modifythe data packets including network protocol headers or payload fields.
- Methods which modify the structure of packet streams.
- Hybridsteganographicmethods(HB)thatmodifiesboththecontentas well as timing &ordering of packet.

Existing methods available for Network steganography:

- SkyDe : Skype Hide
- SCTP Steganography: Multistreaming-basedmethod
- LACK (Lost Audio PacketsSteganography)
- PadSteg: Introducing Inter-ProtocolSteganography

Performance Measure:

Every network steganographic methods has the following attributes –

- *Steganographic Bandwidth*: This term specifies the amount of secret data that can be sent per unit time while using a particularmethod.
- *Un-detectability*: Un-detectability is the inability of a stego-file to get detected when passing through the transmission medium. To detect the possibility of an stego-file, the statistical properties of the captured data are analyzed and then compared with values suitable for thatcarrier.
- *Robustness*:Robustnessspecifiestheamountofalteration a stego-file can undergo withoutitssecretdatabeingcompromised.Steganographicmethodwhich is highly robust (tolerant)and difficult to detect and also offering highbandwidth can be considered as a good steganographicmethod.

2.4 Goals of Steganography

The primary goal is to hide data. Also, there are several other goals helps in analyzing the strength of the steganographic technique used.

This include:

Undetectability (imperceptibility): This is the most important parameter which must be always satisfied. It resembles the strength to avoid detection, i.e., where the naked human eye fails to notice it. But, there are techniques which do not change the image to be detected by naked eye but still it alters the image which can be detected by the statistical tests. Steganography techniques which are undetectable to the human eye or by the statistical attacks can be considered as 'secure'.

Robustness: This parameter indicates the strength of the steganography technique being used to tolerate various visual and statistical attacks. It should combat various manipulations done on image like rotating of image, cropping of an image. The image watermarks is considered as a best example for this purpose.

Payload capacity: It refers to the maximum amount of data that can be concealed and retrievedsuccessfully. In case of Watermarking, it has to hide very small amount of information (like a signature) but in case of steganography amount of information to be hidden may be little large, so anadequate embedding capacity is necessary.

2.5 Feature Extraction andFuzzy Preprocessing In Steganography

A set of features is extracted from the stego-image (input data) in the feature extraction process. It is a form

of dimensional compression. Extraction of the chi-square probability as the statistical feature and the Euclidian norm as the visual feature is done. The same features are retrieved from the cover image. The features are extracted using the following methods [1,8].

(a) Chi square probability: This method proposed by Wetsman and Pitsfield [4]to extract this feature. It is done on the basis of the predicted and examined frequencies of the image pixels.

(b) Euclidiannorm: The input features are subjected to fuzzy processing. Based on some analysis it is found out that bell-shaped function can well approximate our input space. Suppose that x and y is the input features. The bell-shaped functions variesas per the parameters which resembles various forms of membership functions [4].

3. OUR WORK

After extensive study of the theory of steganography as well as fuzzy neural networks, we started to the implementation of some methods with slight modifications i.e. improvement in accuracy to get better performance and clear idea about such methods. We will try to use image and audio as cover media. We build a web application which accepts the image as an input from the user. The secret message which is going to be embed in the image is also taken as an input from the user. Then the first phase of our system is Steganography is done. The next phase is the Hybrid fuzzy neural network which will work partially and we will continuously work on it. We have also provided 2-layer security in our system. The first layer consists the AES algorithm for encrypting the secret message and the second layer is of OTP authentication which is implemented at receiver side.

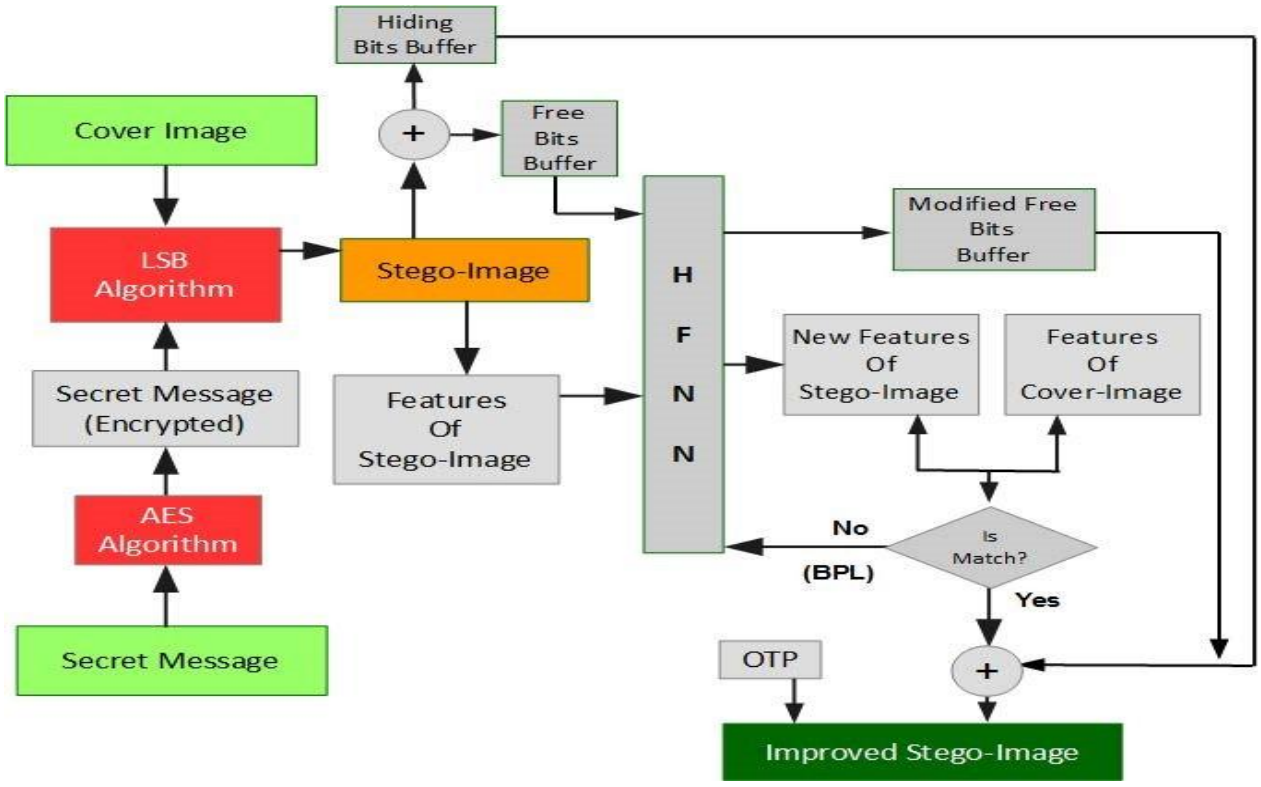

Figure 1. Diagram showing interconnection between different components of the Steganography system using HFNN

3. DISCUSSION

Although Steganography is in use literally for thousands of years but it's a number of forms provide us a chance to continuous research and improvement in this field. In audio steganography, we can try to implement PCM technique. In image steganography, we can explore LSB encoding technique. suitablesteganographic

algorithm for color images. Video and Network Steganography techniques explored theoretically but not practically. Those are also open research area for us.

4. CONCLUSION

Within this paper, an overview of steganography is given with explanation and basic principles and analysis of using this technique for various cover media formats, and lastly the future system of using steganography in image and audio. There are various special techniques for embedding data into variousdigital mediums, and each medium possess its own strengths and weaknesses. The LSB encoding technique considered especially faster and easier, whereas the transform domain and feature modification methods, are considered somewhat powerful than it. Other future advancements are rising to search for new methods which can be used for hiding as well as retrieving secret data.

REFERENCES

[1] Saleema A., Dr. T. Amarunnishad, "A New Steganography Algorithm Using Hybrid Fuzzy NeuralNetworks",InternationalConferenceonEmergingTrendsinEngineering,Scienceand Technology(ICETEST),ScienceDirect,2016.

[2] VipulaMadhukarWajgade , Dr. Suresh Kumar, SGT Institute of Technology And Management, Gurgaon, Haryana, India, "Enhancing Data Security Using Video Steganography", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 4, April2013.

[3] Christy.A.Stanley, "Pairs of Values and Chi Square Attack", Department of Mathematics, Iowa State University, May 1, 2005Fachinger, J., 2006. Behavior of HTR Fuel Elements in AquaticPhasesofRepositoryHostRockFormations.NuclearEngineering&Design236,54.

[4] Westfeld, A., Pfitzmann, A., 2000. "Attacks on Steganographic Systems", 3rd International Workshop, Lecture Notes in Computer Science, vol. 1768. Springer-Verlag, Berlin, Heidelberg, NewYork.

[5] Cvejic, Nedeljko, Department of Electrical and Information Engineering "Algorithms for audio watermarking and Steganography", Information Processing Laboratory, University of Oulu, Finland 2004.

[6] Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing", ThirdEdition.

[7] Petticolas, F.A.P. Anderson, R. J. Kuhn, M. G. 1999, "Information Hiding-A survey", ProceedingsoftheIEEE,SpecialIssueonIdentificationandProtectionofMultimediacontent 87, 1062-1078.

[8] S Sivanandam, S Sumathi, "Introduction to neural networks using matlab6.0".