ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

Use of Visual Cryptography and Neural Networks to Enhance Security in Image Steganography

K.S. Seethalakshmi

P.G. Student, Department of Computer Science and Engineering, RV College of Engineering, Bangalore, India

ABSTRACT: As a result of widespread use of communication medium over the internet, information security has become the area of concern. In the field of internet, the main issue is the data security. Image steganography is concerned with sending secret message while hiding its existence itself. Cryptography is not concerned with hiding the existence of a message, but it means a process called encryption. In order to achieve a better level of secrecy, a message is encrypted before being hidden in a message. Hence, after applying encryption, image steganography embeds the secret message in a cover, such as a digital image file. Steganalysis deals with the whole field of defeating steganographic techniques. Steganography is a constantly evolving field as advances in steganography are usually countered by advances in steganalysis. Thus image steganography alone is not sufficient for providing data security. Visual cryptography is a popular technique to protect image based data. It splits the image into shares during encryption process and these shares are stacked to get back the original image during decryption. So, no special decryption algorithm is needed, just human visual system would suffice. Hence in order to achieve higher level of security, both image steganography and visual cryptography are required. Neural networks are used to identify the best locations in cover image to embed the secret data, improving quality of the image.

KEYWORDS: Cryptography, visual cryptography (VC), steganography, neural networks (NN), radial basis functions(RBF), Integer Wavelet Transformation(IWT)

I. INTRODUCTION

Steganography is a technique of hiding secret message while covering it's existence. The secret message can be audio, video, text, images etc. Electronically, in steganography secret message is converted into binary form and is then embedded into the cover file which is an image or audio file. The resulting output image is called as stego image. In image steganography the cover image is an image file.

Cryptography is about constructing and analyzing protocols that prevent public from reading secret messages. Steganography is about hiding the existence of the secret message. In other words, it involves hiding the information in such a way that it appears no information is hidden at all. Hence, when we combine cryptography with steganography, it results in a powerful tool which enables the people to transmit sensitive data over the internet securely, without possible eavesdropper even knowing that there is a form of communication. Neural networks are used to identify the best locations with high energy coefficients so that embedding is done over those locations. By doing so, the quality of the image would be as good as the original image. Visual cryptography is a unique technique where data is hidden in images and these images are split into number of shares during encryption. During decryption, these shares are overlapped into one another to get back the original image. No special decoding schemes are needed, just human visual system is sufficient. Thus by combining image steganography and visual cryptography, it adds lot of challenges to identify encrypted data for the intruders, thus providing additional layer of security for the secret data.

This paper is organized into 4 sections. Section 1 contains introduction about cryptography, image steganography, visual steganography, neural algorithm. Section 2 contains literature review on selected papers on visual cryptography and image steganography. Section 3 contains description of proposed system. Section 4 contains description of algorithms. Finally paper would be concluded

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

II. LITERATURE SURVEY

Steganography especially when combined with cryptography is most powerful tool which enables people to transmit sensitive data over internet securely without possible eavesdropper even knowing there is a form of communication. In this paper Yogita Patil [1] demonstrates the use of genetic Algorithm, image steganography and Visual Cryptography for Data Hiding in image for Wireless Network. Methodologies followed are i) Data Encryption using any Encryption algorithm ii) LSB Steganography is used for hiding the secret data in the cover image iii) genetic algorithm is used to reshuffle the modified image bits, so as to ensure better security iv) visual cryptography is applied at the end to secure transmission of the image over the internet. Advantages are i) this project resulted in better results in terms of image quality and steganalysis, ii)security features are highly optimized as genetic algorithm is used for reshuffling the bits iii) visual cryptography ensures the secured transmission of the image over the internet. Future scope would be i) could be towards adding public/ private key for encryption ii) face recognition facility for user to introduce more security

S.Premkumar and R.Swathiramya [2] prove that optimal Contrast Grayscale visual cryptography with modified multi-secret sharing for secure application. Methodology involves i) hiding the secret information in the edges rather than the smooth areas of a cover image ii) Multiple Base Notational Systems (MBNS) is used. Advantages are i) MBNS serves more security, best values in terms of performance, quality metrics in comparison BPCS, PVD. Future scope would be towards adding face recognition facility for user to introduce more security

Moushmee Kuri and Dr. Tanuja Sarode [3] combined steganography with Random key share overlapping(RKO) technique for Visual Cryptography . Methodology involves i) LSB method is applied for image steganography ii) RKO technique is used to split stego image into random share and key share at the sender side. At the receiver side i) random share and key share are overlapped using XOR method to form single image or stego image ii) reverse image steganography is applied to get back the original image. Advantages are i) perfect reconstruction property, the revealed data and the cover image are exact replica of the original ii) can be used by forensic and security investigators to hide/detect suspicious data iii) less storage & less amount of computation time iv) VC ensures it's impossible for the attacker to even guess that the transmitted shares would contain some hidden data. Future scope would be towards adding user authentication using password and/or photo.

Monu U. Ragashe1 and Sneha M. Ramteke2 [4] did good research on image steganography and visual cryptography algorithms and their findings are listed under the title "Combine use of steganography and visual cryptography in computer forensics". Various steganographic techniques explained are LSB, Dynamic Compensation LSB , Video, audio, image, text steganography types. Various visual cryptographic techniques explained are threshold Image Hiding Scheme, Image Size Invariant VC, joint visual cryptography and waterfall (JVW) method, region incrementing visual cryptography(RIVC). Advantages are i)The importance of Steganography and VC with respect to security are highlighted ii) better performance of visual cryptography with respect to cryptography is explained. Future scope is to invent some more efficient and effective image Steganography and VC techniques.

S. R. Navale, S. S. Khandagale, R. A. Malpekar, Prof. N. K. Chouhan [5] came up with an approach for Secure Online transaction using Visual Cryptography & Text Steganography. Methodology involves nformation submitted by the consumer to the online website at merchant's site is minimized by providing only minimum information that will only verify the payment made by the consumer from his account. This is accomplished by the introduction of a central Certified Authority (CA) and combined application of Steganography(uses ASCII code)and visual cryptographic (k, n) threshold RG-based VC technique. Advantages are i) minimizes consumer information sent for TRANSACTION OF FUNDS to the online merchant's website ii) prevents illegal use of consumer information at merchant's website iii) Presence of a fourth party, CA, enhances consumer's fulfilment and security. Future scope would be i) he payment system can also be extended to internet or physical banking ii) shares may contain consumer image or signature in addition to consumer authentication password

S. R. Khonde, Dheeraj Agarwal and Shrinivas Deshmukh [6] propose "Online Payment System using BPCS Steganography and Visual Cryptography". Methodology involves providing least information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a central Certified Authority (CA) and combined application of BPCS Steganography and Visual Cryptography. LinkGuard Algorithm is also used. Advantages are i) provides customer data privacy, prevents misuse of data at merchant's side ii) BPCS Steganography is highly effective against eavesdropping and has a high information hiding capacity as compared to

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

traditional steganography approach iii) prevention of identity theft and customer data security iv)consumer satisfaction and authorized merchant-bank interaction. Future scope is to apply the proposed method can be applied for E-Commerce with focus area on payment during online shopping as well as physical banking

III. PRAPOSED SYSTEM

The proposed model for security enhancement for image steganography using visual cryptography and neural networks is as shown in Fig 1.

The main phases during encryption are as below.
i) the secret message is encrypted using AES encryption algorithm
ii) the cover image is resized and divided into 8*8 blocks
iii) IWT is applied on the cover image to identify the energy co-efficients
iv) Neural network algorithm uses the RBF function to identify the high energy coefficients to embed the secret data into the cover image
v) Secret data is embedded into the identified high energy coefficients using LSB embedding technique
vi) Inverse IWT is applied to negate the effects of IWT on the cover image
vii) Data re-arrangement is done so as to bring the image to original shape

The secret message could be in the form of text which is converted into binary form. AES algorithm is used to encrypt the secret message. The cover image, which is used to hide the secret bits, is resized into a standard size and is divided into (8*8) blocks. IWT is applied to identify the high energy coefficient. These high energy locations would be less noisy and hence the quality would be better if secret message bits are stored here. LSB embedding ensures that the image visibility is not affected due embedding. LSB Steganography has high embedding capacity and low computation complexity, in which a secret binary sequence is used to replace the least significant bits of the host medium. Later on inverse IWT, data rearrangement is applied to get back the cover image in original shape and form. Visual cryptography is applied in which the cover image is divided into two shares and send to the data base. The alternate pixel information is stored in different shares.

At the receiver, when the two shares of the image are received, inverse visual cryptography is applied, in which these two shares are overlapped to get back the single image. Later, de embedding is performed followed by decryption to get original secret data.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

IV. FIGURES

Below Fig. 1 depicts the architecture of encryption and decryption phases.

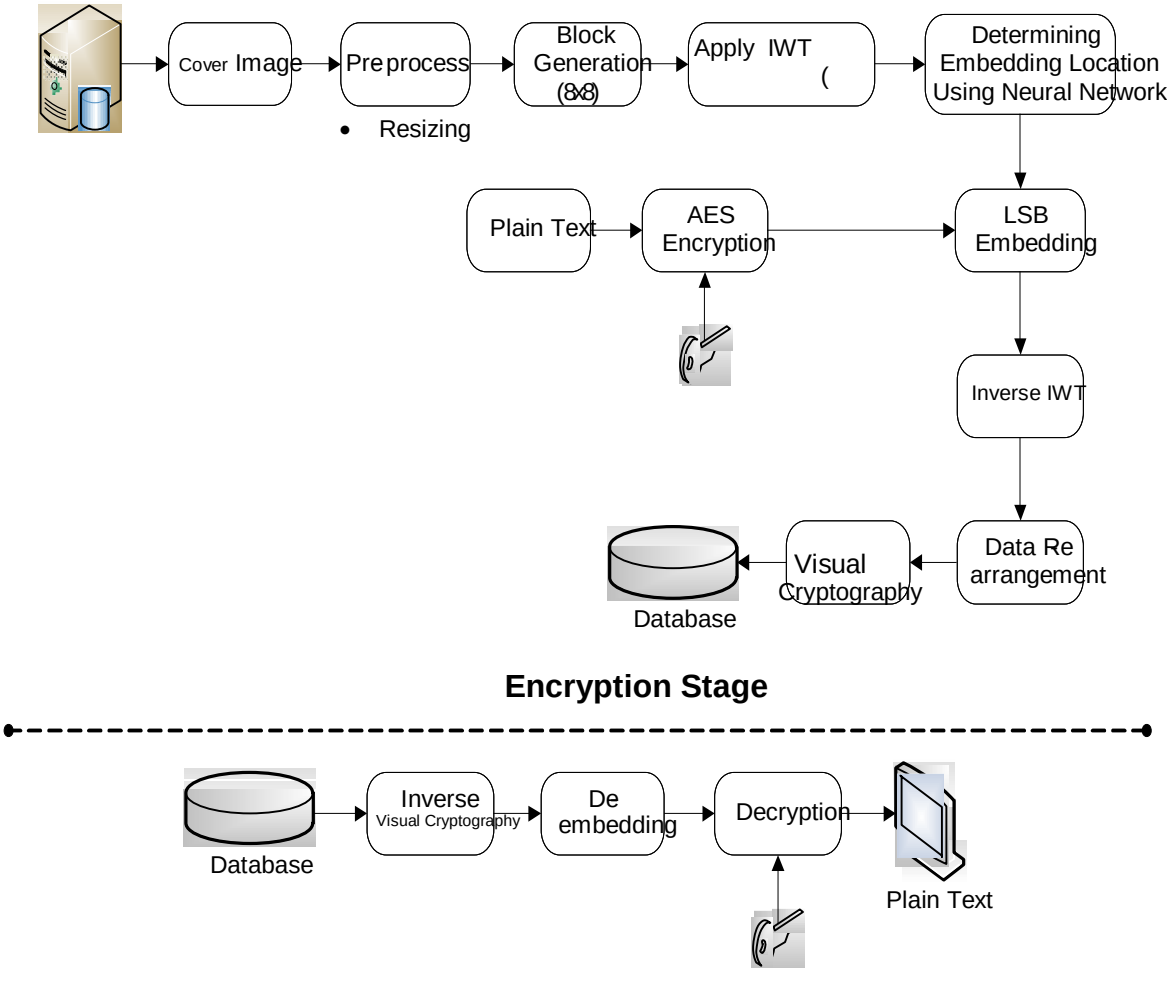


Figure 1 : Encryption and decryption block diagram

V. ALGORITHMIC DESCRIPTION

The praposed system uses two main algorithms during encryption stage

Encryption stage

i) LSB embedding using RBF functions of neural networks

a) read encrypted secret image
b) read the cover image for hiding the secret data, resize the image, form 8*8 blocks
c) find out energy coefficients of the image by applying IWT
d) find out high energy coefficients using RBF functions of the neural network

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

e) using LSB embedding encrypted secret data is embedded into the cover image

ii) Visual cryptography

a) read the output of algorithm 1 as input

b) image is converted into binary image

c) alternate pixel information of the image is read and stored into different shares

d) these two shares are transmitted over the network

5.2 Decryption stage

Below are main stages during decryption

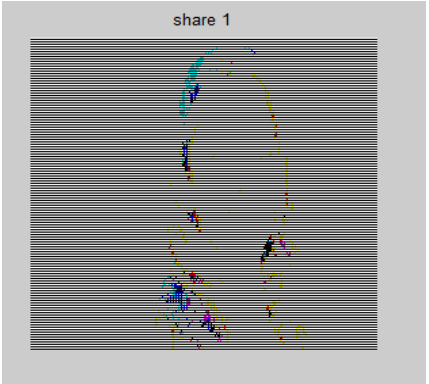
i) Inverse visual cryptography is applied in which two shares having different pixel information in each are overlapped to form one single image. As we can recall, alternate pixel information is stored in different shares.

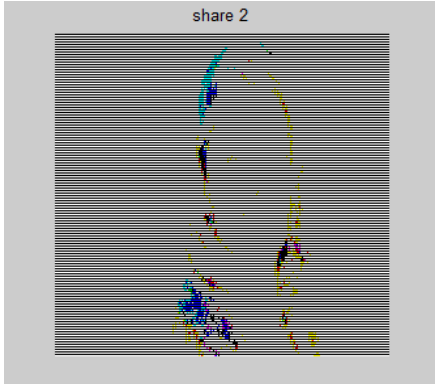
ii) De-embedding is performed, in which secret image which was embedded during LSB embedding is retrieved back

iii)decryption is performed on the output of above step, so as to get back the original secret information.

VI. EXPERIMENTAL ANALYSIS

PSNR value is used to measure the effectiveness of the image steganography. During the experiment, the secret message with 16 alphanumerical characters are used and results are verified. The best PSNR value obtained is 29.52. Below is an example. Similarly many different host images are tried and resultant PSNR was almost same. The secret meassage used was “asdfghjk12345678”. The host image and embedded images, two shares using VC are as below





VII. CONCLUSION

The algorithm proposed here results in high security and image quality. Visual Cryptography ensures the secure transmission of image over the internet. The future scope would be

i) to add private or public key for encryption

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

ii) increase number of shares in visual cryptography to compare the improvement in quality

VIII. ACKNOWLEDGEMENTS

I deeply express my sincere gratitude to **Dr. K. N. Subramanya**, Principal, R.V.C.E, **Dr. Shobha G**, Head of Department, Computer Science & Engineering, R.V.C.E, my guide **Usha B.A**, Assistant Professor, Department of CSE, R.V.C.E for their valuable guidance and support for this project.

REFERENCES

[1] Yogita Patil , "Use of Genetic Algorithm and Visual Cryptography for Data Hiding in image for Wireless Network", International Journal of Computer Applications (0975 – 8887) Volume 113 – No. 1, March 2015

[2] S.Premkumar, R.Swathiramya, "Optimal Contrast Grayscale Visual Cryptography with Modified Multi-secret Sharing for Secure Application", Int. Journal of Engineering Research and Applications, ISSN : 2248-9622, Vol. 4, Issue 4(Version 5), pp.103-106, April 2014

[3] Moushmee Kuri, Dr. Tanuja Sarode, "Steganography Combined with RKO Technique for Visual Cryptography", IJCAT International Journal of Computing and Technology, ISSN : 2348 – 6090, Volume 1, Issue 4, May 2014

[4] Monu U. Ragashe1, Sneha M. Ramteke2, " Combine use of steganography and visual cryptography in computer forensics", Discovery, Volume 18, Number 51, May7, 2014

[5] S. R. Navale, S. S. Khandagale, R. A. Malpekar, Prof. N. K. Chouhan, "Approach for Secure Online transaction using Visual Cryptography & Text Steganography", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, www.ijert.orgIJERTV4IS030775 (This work is licensed under a Creative Commons Attribution 4.0 International License.) Vol. 4 Issue 03, March-2015

[6] S. R. Khonde, Dheeraj Agarwal, Shrinivas Deshmukh, "Online Payment System using BPCS Steganography and Visual Cryptography", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012): 3.358, Volume 3 Issue 11, November 2014