International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 22 (2018) pp. 15477-15483
© Research India Publications. http://www.ripublication.com

Image Steganography using Password Based Encryption Technique to secure e-Banking Data

Atanu Sarkar[1], **Sunil Karforma**[2]
[1,2] Dept. of computer Science,University of Burdwan,West Bengal,India
Email corresponding author: atanu.sk@gmail.com

Abstract

e-banking is the essential financial transaction system via online. It is required to keep the financial data intact and secure from the intruder. In this paper we have applied password based encryption technique on image Steganography to secure e-Banking data. Customer should require registration through personal data along with user_Id and password to access one's account and it requires eight characters for password preparation. Image is segmented into eight non overlapping blocks for embedding secret information. Eight characters are required to form block key for eight consecutive blocks. Message bits are encrypted with block key using XOR method and embedded eight bit per pixel into RGB cover image. On the receiver side images are authenticated by password and retrieve message using XOR technique.

Keywords: Steganography, XOR, LSB, IQM

INTRODUCTION

We are living in information age where large amount of valuable information is communicating through internet. Our goal is that how to secure the information from unwanted intruder. In this digital world people are getting habituated with e-Banking transaction through internet. People are getting various services through e –Banking such as opening an account, money transfer from one account to another account, bill payment, product purchasing etc. So, customer information has to be secured during the transaction through internet. Cryptography and steganography are the two method by which we can provide the security of information.

Cryptography [1, 2], a word with Greek origins, means "Secret writing". We use the term to refer to the science and art of transforming messages to make them secure and immune to attack. Although in the past cryptography referred only to the encryption and decryption of messages using secret keys, today it is defined as involving three distinct mechanisms : symmetric-key encipherment, asymmetric-key encipherment and hashing.

Steganography [3,4] is an art of concealment of information through different cover media such as audio, video, text and image. Image steganography is a method where large amount of information is stored into images keeping its visual quality intact with original image. Image steganography is applied in two domain – spatial domain and frequency domain. Our proposed method is focused in spatial domain with colour image.

LITERATURE REVIEW

Simple LSB substitution method

There are lot of research work has carried on LSB method [6, 7].Chan al et al. [5] has proposed a simple LSB substitution method. In this LSB method secret data are directly embedded into least significant bit positions of cover image. Major advantageous of LSB method is that it is easy to implement and archive high capacity. But one of the main drawback of this method is it is vulnerable to slight image manipulation like cropping, compression.

Manjula et.al [6] has applied hashing technique to embed the secret with different bit position into colour cover image. They have used 2-3-3 bit for red, blue and green pixels. They have archived good capacity of secret bit as well as slight increase of security rather than simple LSB method.

Sarkar and Karforma [7] have tried to improve the security level by applying a new pixel selection technique. Here embedding has started at middle region of an image and successive diagonal pixels have selected to form quadrilateral through which secret data are inserted into pixels.

Pixel value differencing method

Wu and Tsai [8] have proposed high capacity embedding method using pixel value differentiation method. In this paper pixels image are divided into some blocks containing two consecutive pixels. Calculate the intensity difference between two consecutive pixels and modifies the pixel differences of each block (pair) for embedding data bit. A larger pixel value difference allows greater modification in original pixel. In extraction phase, original range table is necessary to portioned of stego image by the same method as used to cover image.

Tsang and Leng [9] have proposed a steganographic method based on PVD and perfect square number. In this paper before embedding secret data, the function Nearest_PerfectSquare () is defined to find the nearest perfect square number for difference value of two consecutive pixels. The function Nearest_PerfectSquare () returns the nearest perfect square number which is the range number of difference value of two consecutive pixels. According to range number, the secret data is embedded into the cover image by the embedding procedure. This method has achieved high capacity than Wu and Tsai method.

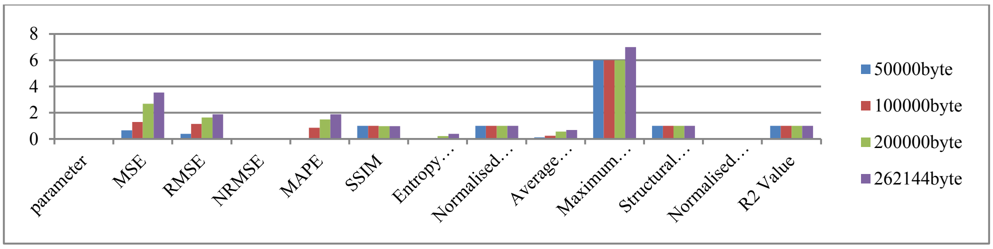

Figure 5. 2D column analysis of various image quality parameters for Leena image.

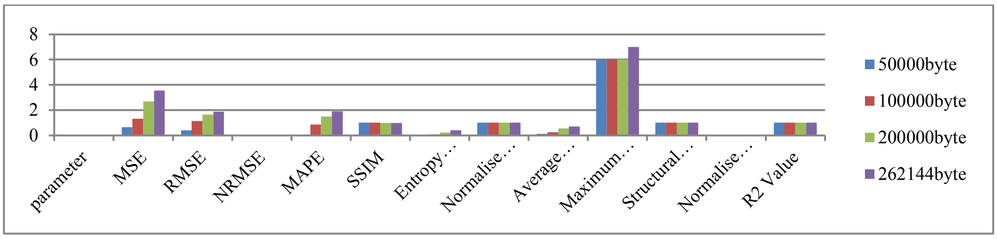

Figure 6. 2D column analysis of various image quality parameters for Peeper image

Table 4. Capacity comparison of proposed method with existing method

Image name & size	PVD[8]	GLM[10]	PMM[11[	Proposed Method
Leena 512×512	50960	32768	90630	262144
Peeper 512×512	50685	32768	93184	262144

Table 5. PSNR comparison of proposed method with existing method

Image name & size	PVD[8]	GLM[10]	PMM[11]	Proposed Method
Leena 512×512	41.79	35.20	33.83	42.60
Peeper 512×512	41.73	34.60	33.86	42.64

CONCLUSIONS

Our Block based Steganography method has achieved better result than existing one in terms of PSNR and capacity. Our proposed method will be applied with two aspects. First one where high security data are transacted through internet we can embed small amount of message (less than 100000) information into stego image. But where large amount information (less secure) transacted through internet such as print saving statement, we can apply our proposed method with message size greater than 1 lakh byte. Our proposed method can be applied on document associated with e-governance, e-commerce, e-learning etc where valuable information is transacted through internet.

REFERENCES

[1] Forouzan B. A., "Data Communication and Networking ",MacGraw Hill Education (India) Private Limited.

[2] Provos N, Honeyman P, "Hide and Seek: An Introduction to Steganography", IEEE Security and Privacy, Vol. 1, No. 3, pp. 32–44,2003 .

[3] Kumar A, Pooja M. K., "Steganography a Data Hiding Technique", International Journal of Computer Applications, Vol-9,No-7,Nov 2010.

[4] Bender W, Gruhl D, Morimoto N, Lu A., "Techniques for data hiding", IBM Systems Journal Vol. 35(3-4),pp. 313-336, 1996.

[5] Chan. C.K. and Cheng L.M.," Hiding data in images by simple lsb substitution". Pattern Recognition, 37:469–474, 2004.

[6] Manjula G.R.,Danti A.,"A novel hash based LSB (2-3-3) image Steganography in spatial domain", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol. 4, No 1, February 2015 .

[7] Sarkar A., Karforma S., " A new pixel selection Technique of LSB based steganography for data hiding",IJRCS, Vol-5,Issue-3,pp.12-125,March 2018.

[8] Wu C.D., Tsai H.W., "A Steganographic method for images by pixel-value differencing", Pattern Recognition Letters, Vol. 24, pp. 1613-1626, 2003.

[9] Tseng W.H. and Leng S.H. , "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number ", Hindwai Journal of Applied Mathematics, Vol. 2013, 2013.

[10] Potdar V. and Chang E. Gray level modification steganography for secret communication. In IEEE

International Conference on Industria lInformatics., pages 355–368, Berlin, Germany, 2004.

[11] Bhattacharyya S. and Sanyal G., Hiding data in images using pixel mapping method (pmm). In Proceedings of 9th annual Conference on Security and Management (SAM) under The 2010 World Congress in Computer Science, Computer Engineering, and Applied Computing(World Comp 2010), LasVegas,USA, July 12-15,2010.

[12] Kaur R. and Pooja , “XOR Encryption Based Video Steganography”, IJSR, Vol. 4, Iss. 11,pp. 1467-1471,Nov 2015

[13] Panghal S., Kumar S. and Kumar N., “ Enhanced Security of Data using Image Steganography and AES Encryption Technique”, *IJCA Proceedings on Recent Trends in Future Prospective in Engineering and Management Technology* RTFEM 2016(1):1-4, July 2016

[14] Deshmukh E., Dangle J., Ghadi S, Kewat S. and Shewale K, “Image Steganography-Hiding Data within Image ”, Vol.5,Iss.1,jun 2016.

[15] Varnan S. C., Jagan A., Kaur J., Jyoti D., Rao S.D., “Image Quality Assessment Techniques in Spatial Domain”, IJCST, Vol. 2, Iss. 3, September 2011.

[16] Memon F.,Unar A,M. and Memon S.,”Image Quality Assessment for Performance Evaluation of Focus Measure Operators”,MURJET, Vol. 34, No. 4, October 2015.