International Journal of Engineering & Technology, 7 (2.24) (2018) 239-242

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Computational Approach of Highly Secure Hash Algorithm for Color Image Steganography Using Edge Detection and Honey Encryption Algorithm

K.Dhanasekaran[1], P.Anandan[2], A.Manju[3]

[1]Department of I&C Engineering, Mailam Engineering College, Mailam
[2]Vel Tech MultitechDr.RangarajanDr.Sakunthala Engineering College, Chennai.
[3]School of EEE, SASTRA University, Thanjavur.

Abstract

Securing and transmitting data through images without being hacked is important in stegnography. Identification of the hidden data without the knowledge of appropriate algorithm is beyond bounds. In this paper we propose a highly secure algorithm for hiding data using advanced encryption algorithm, wherein the hidden data could be identified by canny edge detection and appropriate hash algorithm method. Color images are converted into grayscale images and edges are retrieved and honey encryption algorithm is used for encoding and decoding process. Simulated results in Matlab exhibits high security of the proposed method over other methods on comparison.

Keywords: *Steganography, Advanced Encryption Algorithm, Encoding And Decoding.*

1. Introduction

Steganography is a method to hide data within the carrier signal. Steganos stands for secret and graphy stands for writing. Images, videos and audio files are used to hide the message, called as cover medium. Secret data is inserted in the space created by removing redundant bits in the cover media. Quality of video depends on the redundant bits available for hiding [2][3][19].
Many algorithms for encryption like DES, RSA, Blowfish, AES to secure the data against brute force attacks are available, but due to insecure block cipher and weak key problems, detection of attacks is not that winning[6][18]. In this paper we propose a honey encryption algorithm, such that the attackers employing a brute force attack gains no information by guess and checking for key.
In this paper information is hidden using honey encryption algorithm and hash function. Main advantage of this method lies in the number of bits produced as outputs. MD5 (message digest 5) method produces an output of 128 bits for a message of 2^{64}-1(Maximum message size), but the proposed method has unlimited message size and produce output upto 512 bits. Besides, decoding of hidden data uses less than 64 bits in MD5 [13], upon 256 bits in the proposed method for enhanced security. In apart we can hide different types of files format like video, audio and an images etc. Recent interests of research fraternity include employing video in stenography [11]. This provides an additional security against hacking owing to the complexity of videos compared to audio/data.

2. Edge Detection

Edge detection forms a crucial part in image processing asit identifies the points of sharp changes and organizes into a set of curved lines segments [7]. For the image formation model in general, discontinuities in images brightness are likely to correspond to Discontinuities in depth, surface orientation, Changes in material properties andVariations in scene illumination.
Ideally, edge detector is used to find the boundaries in an image, discontinuities in surface orientation as well as curves in the surface marking of the boundaries. Successful edge detection implies retrieval of all the data from the original images [7],which is herculean in case of real images.
Edge detection is usually performed by Search- and Zero-crossing based methods, involving first order derivative and second order derivative expressions respectively [15].
Prior to the measurement of edge strength noise reduction is done by smoothing process, where filters like Gaussian smoothing filter is employed.Edge detection algorithm is highly sensitive to noise, as it implies false edges when the intensity value changes. In order to avoid this setback, canny method introduces appropriate filtering making it expensive. Canny edge detection is a multi-stage algorithm to detect wide range of edges in images [16].Despite the cost involved in the algorithm, advantages in canny edge detection, namely using probability for finding error rate, localized and response, improving signal to noise ratio, better detection, insensitivity to noise are manifold making it viable.

3. Secure Hash Algorithm

Hash technique is processing ofleast significant Bit using hash principle for steganography[8-10]. Main aim is to hide the information in a particular image and then extracting the secret information by using a stegnokey. In steganography, the LSB insertionis to change the data in cover image in their lower bits, making it invisible. Firstly message file is embedded with cover image and again the file is extracted [8]. Cover image consist of set of pixels and secret information hidden in these frames as payload. Encoding is the process of hiding the data in the image

and decoding is retrieving data by the terms of decoding [10]. Generally for hash value a varying size input is applied and in turn return a digital string of fixed digital value as output. Hash function used to find large files which are duplicated. Hash function can expressed as,

$$X=Y\%Z$$

Where,
X=position of bit in LSB within the pixel,
Y=position of individual hidden image pixel,
Z=number of bits in LSB.
Imagesare created by pixels, and when indicated by colors RED, GREEN and BLUE, are referred as RGB. Each pixelindicates one bit data with the density of color. First bit is referred as MSB and last bit is referred as LSB bit. This LSB bit is meant to encrypt the data within the image. The distribution of secret message bit is shown in Fig.1.
For example If the message is 11001000 of 8 bits, first 3 bits of message of secret is hidden in LSB of red pixel, next 3 bit is hidden in LSB of Green pixel, and then the last 2 bits are embed in LSB of Blue pixels.
In this paper Advanced Hash algorithm is proposed. Main steps of Steganography are Encoding and Decoding.

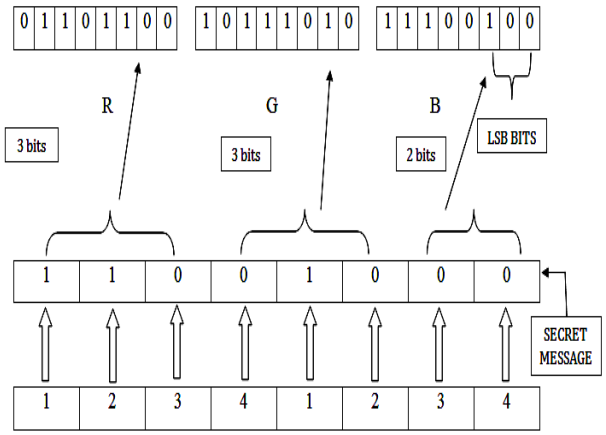


Fig.1: Distribution of secret message bits

4. Encoding Procedure

The advanced Hash algorithm for encoding data is shown in Fig. 2.
Step 1: Secret text is encrypted with honey encryption algorithm and hash function
Step 2: Cipher text is added with cover image
Step 3: Collect the RGB Pixels values from cover images at any size
Step 4: Detect the edges of input images using edge detection algorithm
Step 5: Read the text file, store the data in an array list
Step 6: Encode the image with LSB techniques
Step 7: Replace text data to Red, Green and Blue Pixels of the image.
Step 8: Finally output image containing coded data istransmitted to receiver.

5. Decoding Procedure

Proposed algorithm for Decoding data in image block diagram shown in Fig.3:
Step 1: Read the RGB images that contain encoded information.
Step 2: Input hash key is used with hash function to generate the pattern where data has been stored.
Step 3: Decode the text from images. Values of Red, Green and Blue byte are read one by one, and further stored in the form of string.
Step 4: Output of the text file contains the decided data from the image.

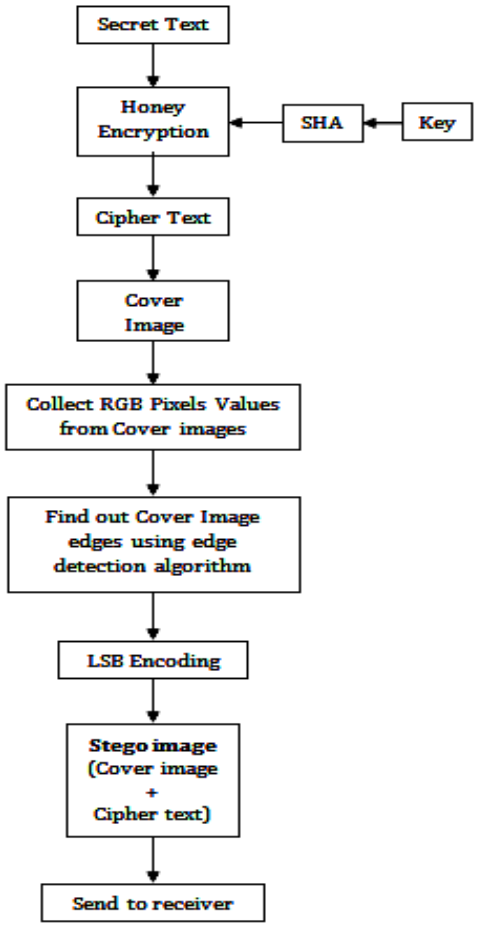


Fig. 2: Block diagram for encoding process

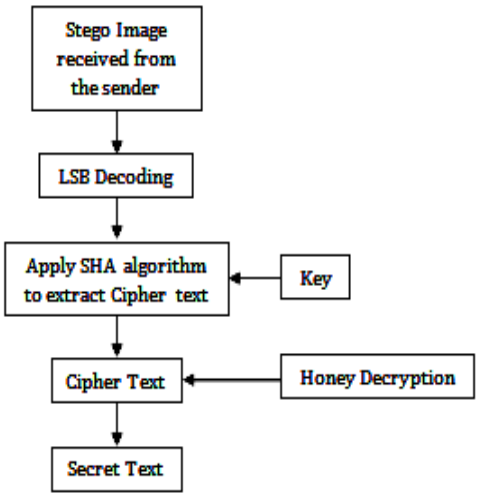


Fig.3: Block diagram for decoding process

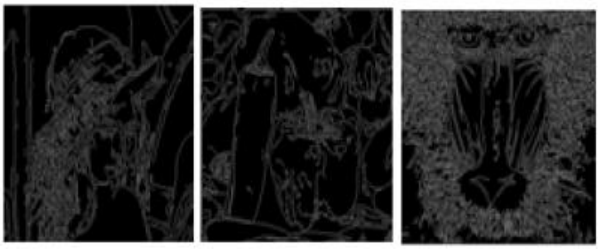
6. Simulation Results

Simulation is performed using three different color images i.e. standard Lena, Pepper and baboon images. Fig.4 shows the original image ofLena, Pepper and baboon images and the size of the images are 512 * 512 and Fig.7 indicates their histograms respectively.Fig.5 shows theedge detection of images using canny edge detection algorithm.

Fig.6 indicates the encoded images which includes hidden data of 2547 bytes.Data is hidden to all the three pixel values. It shows that there is no difference between Fig.4 and Fig.6, as shown in their histograms(Fig.8). We can identify the data hidden in images using their PSNR values of the imagestabulated(Table 1).

Lena.jpeg pepper.jpeg baboon.jpeg

Fig.4: Original images (512 X 512)

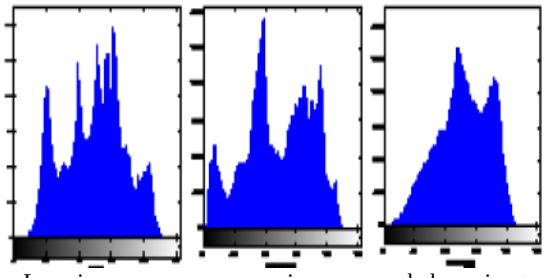


Lena.jpeg pepper.jpeg baboon.jpeg

Fig. 5: After applying canny edge detection algorithm

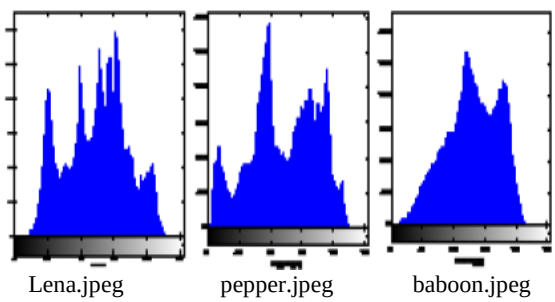
Lena.jpeg pepper.jpeg baboon.jpeg

Fig. 6: Encoded images with text data (2547 bytes)



Lena.jpeg pepper.jpeg baboon.jpeg

Fig. 7: Histogram of original image



Lena.jpeg pepper.jpeg baboon.jpeg

Fig. 8: Histogram of encoded image with text data(2547 bytes)

Table 1: PSNR of the images

S.NO	TEXT DATA	LENA		PEPPERS		BABOON	
		Hash	Advanced Hash	Hash	Advanced Hash	Hash	Advanced Hash
1	849 Bytes	46.7704	47.5599	42.4704	43.7486	44.5141	46.5188
2	1698 Bytes	43.1161	43.7728	39.8468	41.9565	41.4249	44.6801
3	2547 Bytes	40.4854	41.5473	37.9358	40.3967	37.759	43.2978
4	3396 Bytes	39.581	40.0503	36.7382	39.4238	36.3541	42.3406
5	4287 Bytes	38.5342	39.631	35.7352	38.6527	35.1693	41.5895

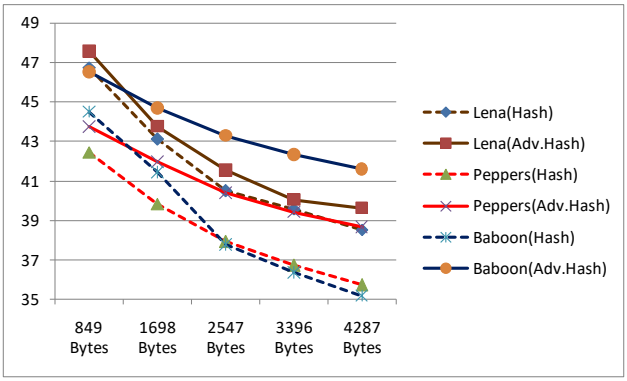


Fig. 9: Graphical results of PSNR value using Hash Algorithm

7. Conclusion

In previous method the data is hidden in blue pixelsonly, whereas all the three basic colors (Red, Blue and Green pixels) are used for hiding data. Advanced hash algorithm gives better results than the previous method asshown in Fig 9 and Fig10.Thismethod produces high quality of stego-images under human visual system. Simulation results shows that text data of 1250 bytes hidden in Lena image gives good results than other two, and if the size of data increases baboon images gives better results. Using advanced hash algorithm givesgood security of hidden images making it difficult to predict the hidden text.

Reference

[1] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Kevitt, “Enhancing Steganography in Digital Images”. Proc. Canadian Conference on Computer and Robot Vision.

[2] Alain,C.Brainos, “A study of Steganography and Art Of Hiding Information,” East Carolina University. International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 4 Issue 8 Aug 2015,Page No. 13760-13764.

[3] 3.Soumyendu Das, Subhendu Das, BijoyBandyopadhyay and SugataSanyal, “Steganography and Steganalysis: Different Approaches”.International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1, June, 2008.

[4] NedeljkoCvejic and TapioSeppÄanen, “Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB

[5] Coding”.Proc. International Conference on Image Processing, Rochester, NY, 641–644.

[6] Domenico Bloisi and Luca Iocchi, “Image Based Steganography And Cryptography”.VISAPP 2007: Proceedings of the Second International Conference on Computer Vision Theory and Applications, Barcelona, Spain, March 8-11, 2007 - Volume 1.

[7] Pund-Dange, S. Desai, C.G. “Secured data communication system using RSA with mersenne primes and Steganography”. Computing for Sustainable Global Development (INDIA Com), 2015 IEEE 2nd International Conference on 11-13 March 2015.

[8] Ziguan Cui, ZongliangGan, Guijin Tang, Feng Liu, Xiuchang Zhu. “simple and effective image quality assessment based on edge enhanced mean square error” Wireless Communications and Signal Processing (WCSP), 2014 Sixth International IEEE conference on September 11 , 2014.

[9] Yu-chi chen, chih-weishiu, gwoboahorng. "Encrypted signal-based reversible data hiding with public key cryptosystem" IEEE article Journal of visual communication and image representation, volume 25, issue 5, July 2014, pages 1164-1170.
[10] MrithaRamalingam, Nor Ashidi Mat Isa, "Video steganography based on integer Har wavelet transforms for secured data transfer", Indian Journal of Science and Technology, Vol 7(7), 897904, July 2014.
[11] Hemant Gupta, SetuChaturvedi, "Video Steganography through LSB Based Hybrid Approach", IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014.
[12] PritishBhotmage et al, "Advance Video Steganography algorithm", IJERA, Volume 4,Issue 6, June 2014, ISSN: 2277 128X.
[13] Falesh M. Shelke1, Ashwini A. Dongre, Pravin D. Soni. "Comparison of different techniques for Steganography in images" International Journal of Application or Innovation in Engineering & Management Volume 3, Issue 2, February 2014.
[14] Quynh Dang, "Recommendation for Applications Using Approved Hash Algorithm", NIST special publication 800-107, Computer security Division, National Institute of Standards and Technology, Dept of commerce, USA, pp. 1-21, 2011.
[15] Zhou Hua and Liu Qiao, "Hardware Design for SHA -1 Base d on FPGA", IEEE International Conference Publications On Electronics, Communications and Control (ICECC), pp.2076-2078, 2011.
[16] N.V Rao, J.TL Philjon, "Metamorphic Crypto- A Paradox between Cryptography and Steganography using Dynamic
[17] Encryption", IEEE Xplore International Conference on Recent Trends in Information Technology, June 2011, pp. 217-222.
[18] Cheng Xiao-hui and Deng Jian-zhi, "Design of SHA-1 Algorithm based on FPGA", IEEE Second International Conference on Networks Security, Wireless Communications and Trusted Computing, (NSWCTC), Vol-1, pp. 532-534, 2010.
[19] Data Hiding and Retrieval, A.Nath ,S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.
[20] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan, Dai Wei-di, "Digital image encryption algorithm based on chaos and improved DES", IEEE International Conference on Systems, Man and Cybernetics, 2009.
[21] Neil F. Johnson, Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, Feb1998, pp. 26-34.
[22] S.V.Manikanthan and T.Padmapriya "Recent Trends In M2m Communications In 4g Networks And Evolution Towards 5g", International Journal of Pure and Applied Mathematics, ISSN NO:1314-3395, Vol-115, Issue -8, Sep 2017.
[23] S.V. Manikanthan , T. Padmapriya "An enhanced distributed evolved node-b architecture in 5G tele-communications network" International Journal of Engineering & Technology (UAE), Vol 7 Issues No (2.8) (2018) 248-254.March2018
[24] T. Padmapriya and V. Saminadan, "Priority based fair resource allocation and Admission Control Technique for Multi-user Multi-class downlink Traffic in LTE-Advanced Networks", International Journal of Advanced Research, vol.5, no.1, pp.1633-1641, January 2017.