International Journal of Engineering and Technology, 2 (2) (2013) 134-139
©Science Publishing Corporation
www.sciencepubco.com/index.php/IJET

An novel architecture for information hiding using HMAC-MD5

L. Agilandeeswari [1*], K. Brindha [2], Stiffy Sunny [3], K. Muralibabu [4]

[1, 2, 3] *School of Information Technology and Engineering, VIT University, Vellore, Tamilnadu, India*
[4] *Department of ECE, Global Institute of Engineering and Technology, Vellore,Tamilnadu, India*
**Corresponding author E-mail: agila.l@vit.ac.in*

Abstract

Communication in digital form has become the part of day today's lifestyle, in certain moment communication is made secret to avoid others from knowing the information. By providing security to the sensitive data it is ensured that the user's data is protected from viewing and accessing by others. In the current discussion about data security, Steganographic algorithm using two mediums has been discussed that involves image based encryption and converting to word file. The stage involving image based encryption uses HMAC-MD5 algorithm along with LSB steganography. LSB technique scatters the secret data which have to be protected over the entire image. Convert the embedded image in word file, so that the secret message is made unavailable to others who try to obtain the file. This method provides greater payload capacity along with higher image fidelity and thus make the proposed system is more robust against attacks.

Keywords*: Steganography, Hashing Message Authentication Code (HMAC), Message Digest Algorithm (MD5), the Least Significant Bit (LSB).*

1 Introduction

Today's environment has lead to excessive use of digital communication channel. The advances digital multimedia such as audio, image and video and the digital network have given rise to serious business threat when valuable data is lost or stolen. When the sensitive information of an organization is exposed that might affect company financial, customer attrition and even the reputation. A potential solution to his problem has been 'cryptography and steganography' which prevents illegal, malicious copying and theft of sensitive data over a digital medium by superimposing data on to the covert image and bringing in a form which cannot be analyzed by steganalysis [1].
Cryptography is one of technique when the sender scrambles the required sensitive information with an encryption key, the receiver with the appropriate decryption key can able to retrieve the original message. This is done because the security in the internet channel is low. Steganography is the process of writing hidden messages into a medium [2]. Steganography is used for secret communication where only the sender and the intended receiver will able predict and retrieve the hidden message [3].
Encryption technique is widely used in to today's environment especially in the image medium. Encryption makes use of the advantage of the human visual system (HVS). The secret messages are encrypted and embedded into a color image and converting it into a word file. The challenges feature is to beat with HVS. This is because of the human visual system able to predict the occurrence of hidden data in the image if the visual perceptibility is high. Thus make sure that the visual perceptibility should be kept as low as possible so that no one other than the intended user will know occurrence of hidden.

2 Related works

In the section of related works, the contribution made related to the work of steganography where data are hidden into an image and extract the data from encrypted media is reviewed. A literature survey in steganography explains how data is encrypted and embedded into a medium and how data is obtained from decoding and decrypting. In each of the related work we summarize the process of the algorithm and limitation of the presented algorithm.
Mishra et al. [5], has proposed LSB Steganographic approach. Data is dispersed using a Plane Cycling methodology where embedding is done on the color image. The image is divided into 8 pixel block and secret message are laid in the

RGB plane of the color image and most of the times B planes remains untouched. Retrieval of data is kept extremely difficult task because of the use of PRNG (Pseudo Random Number Generation). This results in an enhanced security level are visually perceptible change in that image is kept low.
Sharma et al. [6], has proposed two level secure steganography containing audio and image as the mediums for encoding methodology. In the waveform of audio format the secret data are embedded as a bit streams which is further embedded into 24-bit grayscale image using LSB technique. Data is kept secured by using improved plane cycling allowing equal distribution of hidden message over the RGB planes of the cover image. The texture and continuity of the stego-image is found to be unsatisfactory in nature.
Selvi et al. [7], has propose a new LSB Steganography algorithm for hiding the secret data. Data is encrypted on the color image. The sharper region or smooth region of a color image is found using the Laplacian Edge Detection method and data is embedded in those regions. This methodology preserves the statistical and visual features of the cover images and provides lesser payload capacity.
Naqvi et al. [8], has proposed a new technique for enhancing the security of data by using HMAC with MD5 algorithm. A hash function transforms the data of variable length to encrypt data of fixed length using hash value. MAC is a sort of hashing function for which a secret key is used. Message Authentication Code guarantees authentication among the sender and receiver. For the purpose of data integrity and authentication popular cryptographic algorithm, Hashing Message Authentication Code is used. HMAC-MD5 generates the secret key for providing security for data.

3 Proposed algorithm

The proposed system provides two levels of security bringing additional level of protection to covert data. The algorithm uses image and text as the medium to hide the content. The data to be hidden is encrypted and embedded into the image medium later the image medium is further converted into a word file. Thus it provides two levels of protection to the sensitive data.
The Encryption process uses HMAC-MD5 which in turn uses a cryptographic hash function in conjunction with a secret key providing data integrity and authentication and also LSB steganography takes the hidden data and spread it over the cover image to ensure that the occurrence of the secret message should not be known and covert data should not be obtained easily from the cover image. The stego - image is converted into text and stored as a document file format.

3.1 Encoding Algorithm

i. Obtain the secret text which has to be secured.
ii. Using the HMAC-MD5 algorithm encryption is done with the covert data and converted into eight bits-stream of data.
iii. Consider a cover image whose size is larger than the covert data.
iv. The cover image should be divided into 8-pixel block.
v. The secret message which is in bit streams is embedded into a pixel of color image by using LSB Steganography.
vi. Similarly, embed the entire secret text stream into the image, the image which is obtained is the stego-image (i.e. Secret data embedded into the image).
vii. A stego - image which is obtained appears similar to the cover image.
viii. This stego -image is converted into a document file.

3.2 Decoding algorithm

The decoding algorithm is a reverse process of encoding process.
i. Obtain the document file which contains secret information.
ii. With the help of secret keys, open the protected document file.
iii. Convert the document which contains the hidden data into the image file.
iv. Image file which is obtained is stego-image. Divide a stego - image into 8-pixel block.
v. Extract the original data from the 8-pixel block of the stego-image with the LSB technique.
vi. Data which is obtained from stego-image is in encrypted form.
vii. The encrypted data is decrypted using HMAC-MD5 algorithm.
viii. The final data which is obtained is the sensitive data, which is protected via two mediums.

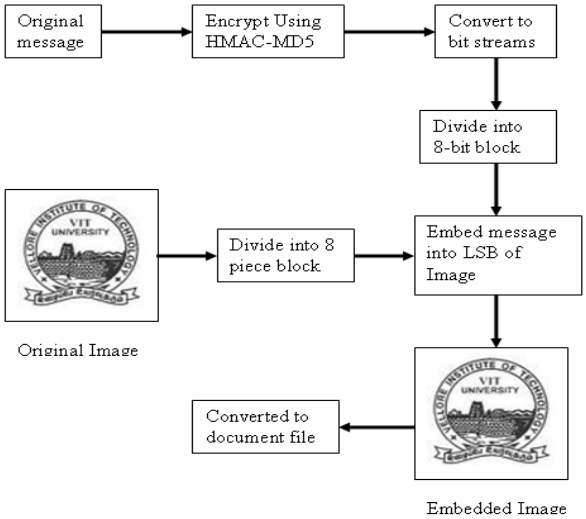

Fig.1: Encoding process of the Proposed Algorithm

4 Results and discussions

The result and discussion based on the proposed algorithm is presented here. The image which is used as cover image is 'vitlogo.jpg'. The fig. 2 is considered to hide the data which are 1024 X 768 pixel image in JPG format. The text which is chosen as the covert data is the speech which was delivered by Mahatma Gandhi in 1942 for 'Quit India Movement' see fig. 3.

Fig.2: Original Image

Occasions like the present do
I am saying and doing today.
therefore, there is any among
vouchsafed to me a priceless
flames of Himsa2 and crying
act now. I may not hesitate ar

Fig.3: Hidden Text

4.1 Based on visual impedance

The visual impedance is carried out between the stego-image and the cover image. An evaluation of the visual inspection of the color image is based on the appearance of the image, texture, continuity between the adjacent pixels of the image, color distortion. The secret data which are to be hidden is taken on the varied characters of 500 to 6000, the data are then embedded into the cover image and the output of the using above characters is shown in the figure 5. The result of the stego-image does not show perceptually significant changes occur in the cover image.

Imperceptibility test is done with PSNR (Peak Signal to Noise Ratio.) The invisibility of the embedded image is measured using PSNR. The PSNR value above 40 is considered reasonable. The experimental value between the cover image and stego-image found to be 63.6 567.

4.2 Based on Size of Embedded Messages

The analysis is based on the size of the embedded message used. From the figure 4 shows that there is an increase in the number of characters used for embedding process. Through the histograms of the stego-image and the original image we can understand the gradual degradation of the image has occurred as the amount of data used to embed into the image increases which reflects through the variation in the histogram. As the number of characters increases in the cover image, there is more number of pixels witness change.

(a) (b) (c) (d) (e)

Fig. 4: Possible number of characters embedded in stego-image. (a) Stego-Image with 500 characters, (b) Stego-Image with 1000 characters, c) Stego-Image with 2000 characters, (d) Stego-Image with 5000 characters, (e) Stego-Image with 6000 characters

4.3 Based on attacks

To test the robustness of the proposed algorithm, various attacks has been made on the stego-image and checks for extracted output as,

4.3.1 Gaussian attack

Gaussian Noise is added on the image with the mean and variance value as '0' and 0.01 respectively. The corresponding image is shown as,

Occasions like the present do
I am saying and doing today.
therefore, there is any among
vouchsafed to me a priceless
flames of Himsa2 and crying
act now. I may not hesitate ar

(a) (b)

Fig. 5: (a) Gaussian Attacked Image (b) Extracted Text.

4.3.2 Poisson Attack

Poisson Noise is added on the stego image. The corresponding output image is shown as,

Occasions like the present do
I am saying and doing today.
therefore, there is any among
vouchsafed to me a priceless
flames of Himsa2 and crying
act now. I may not hesitate ar

(a) (b)

Fig. 6: (a) Poisson Attacked Image (b) Extracted Text.

4.3.3 Salt & Pepper Attack

Salt & Pepper Noise is added on the image with the noise density 'D' as 0.05. The corresponding image is shown as,

Occasions like the present do
I am saying and doing today.
therefore, there is any among
vouchsafed to me a priceless
flames of Himsa2 and crying
act now. I may not hesitate ar

(a) (b)

Fig.7: (a) Salt & Pepper Attacked Image (b) Extracted Text.

4.3.4 Median filtering

By applying median filtering on the stego image is shown as,

Occasions like the present do
I am saying and doing today.
therefore, there is any among
vouchsafed to me a priceless
flames of Himsa2 and crying
act now. I may not hesitate ar

(a) (b)

Fig. 7: (a) Median filter Attacked Image (b) Extracted Text.

4.3.5 Cropping

The cropped stego image and the corresponding extracted hidden text is shown as,

(a)

Occasions like the present do
I am saying and doing today.
therefore, there is any among
vouchsafed to me a priceless
flames of Himsa2 and crying
act now. I may not hesitate ar

(b)

Fig.8: (a) Cropped Image (b) Extracted Text.

4.3.6 Rotation

By applying rotation on the stego image with angle 5° and its extracted hidden text is shown as,

(a)

Occasions like the present do
I am saying and doing today.
therefore, there is any among
vouchsafed to me a priceless
flames of Himsa2 and crying
act now. I may not hesitate ar

(b)

Fig. 9: (a) Rotated Image (b) Extracted Text.

4.3.7 Histogram Equalization

The histogram equalized stego image and its extracted text is shown as,

(a)

Occasions like the present do
I am saying and doing today.
therefore, there is any among
vouchsafed to me a priceless
flames of Himsa2 and crying
act now. I may not hesitate ar

(b)

Fig. 10: (a) Histogram Equalized Image (b) Extracted Text.

5 Conclusion

In this paper an effort has been made to provide two levels of security with image and text as the medium. The secret message is encrypted with HMAC-MD5 algorithm using a secret key, and embedded using LSB steganography of the 8 pixel blocks increase the impedance of stego-image and payload capacity of the secret data. Conversion of the stego-image into the word file format raise the bar of security to a higher level, the results which brings at the end are satisfactory in nature as visually perceptible is low and raised the security level.

References

[1] Ge Huayong, Huang Mingshenga, Wamg Qiana, “Steganography and Steganalysis based on the digital image”, International Congress on Image and Signal Processing, 2011.

[2] M.M Amin, M. Salleh, S. Ibrahim, M.R.K atmin, and M.Z.I. Shamsuddin, “Information hiding using Steganography”, National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, 2003.

[3] S. M. Ashar, T M Shah. Khalid, “Message encryption with image processing”, International Multitopic Conference (INMIC), 2003.

[4] S. K. Moon, R.S. Kawitkar, “Data security using data hiding”, International Conference on Computational Intelligence and Multimedia Applications, 2007.

[5] Amitabh Mishra, Akshay Gupta, D.K. Vishwakarma, “Proposal of a new steganographic approach”, International Conference on Advances in Computing”, Control and Telecommunication Technologies, ASET, Amity University, India, 2009.

[6] Divya Sharma, Abha Tripathi, Agam Gupta Regalix, “A two level message adaptive steganographic approach”, International Conference on Advances in Computer Engineering, 2010.

[7] G.Karthigai Seivi, Leon Mariadhasan, K.L Shunmuganathan, “Steganography using edge adaptive images”, International Conference on Computing, Electronics and Electrical Technologies [ICCEET], R.M.K Engineering college Chennai, India, 2012.

[8] Vivek Tomar, Deepti Mehrotra, Ankur Choudhary, “A Statistical Comparison of Digital Image watermarking techniques”, International Journal of Computer Applications (0975-8887) 3rd International IT Summit Conference, 2012.

[9] Syeda Iffat Naqvi, Adeel Akram, "Pseudo-random Key Generation for Secure HMAC-MD5", Telecom and Information Engineering, UET Taxila, Pakistan, 2011.
[10] M. Kharrazi, H. T. Sencar, and N. Memon, "Cover selection for steganographic embedding," in Proc. IEEE Int. Conf. Image Processing, Oct. 8–11, 2006, pp. 117–120.
[11] K. M. Singh, L. S. Singh, A. B. Singh, and K. S. Devi, "Hiding secret message in edges of the image," in Proc. Int. Conf. Information and Communication Technology, Mar. 2007, pp. 238–241.
[12] B. C. Nguyen, S. M. Yoon, and H. K. Lee, "Multi bit plane image steganography," in Proc. 5th Int. Workshop on Digital Watermarking, 2006, pp. 61–70.
[13] X. Zhang and S. Wang, "Steganography using multiple-base notational system and human vison sensitivity," IEEE Signal Process. Lett., vol. 12, no. 1, pp. 67–70, Jan. 2005.
[14] Y. Wang and P. Moulin, "Optimized feature extraction for learningbased image steganalysis," IEEE Trans. Inf. Forensics Security, vol. 2, no. 1, pp. 31–45, Mar. 2007