Steganography Using AES and LSB Techniques

Aishwarya Pandey
Shri Shankaracharya Technical Campus
Dept. of Computer Science and Engineering
Bhilai, Chhattisgarh, India
aishwarya.smvit@gmail.com

Prof. Jharna Chopra
Shri Shankaracharya Technical Campus
Dept. of Computer Science and Engineering
Bhilai, Chhattisgarh, India
jharna.chopra@gmail.com

Abstract

With rapid growth in the digital market, Steganography is going to increase its importance by which the exponential development and secret communication of potential computer users are also increased over the internet. It can also be well defined as the study of secret invisible communication that generally deals with the different ways of concealing the existence of the communicated message. Usually, the data embedding is obtained in communication such as image, text, voice or multimedia content for copyright and also in military communication for authentication and many other different purposes. In image Steganography, the secret hidden communication is obtained through embed a message into a cover image which is used as the medium to embed message into the image and generate a stego image which is a generated image which is carrying a secret hidden message. In this paper we propose a novel method hide secret information in combination of AES and LSB technique. The image quality are selected by the users and based on that the secret messages length are decided. Hence user has full right to select any size output based on requirements.

Keywords— *Data hiding, Steganography, Cover image, cover writing.*

I. INTRODUCTION

Steganography word is originally from two Greek words Steganos which means Covered and Graptos means writing and which literally means “cover writing”. Usually steganography is also known as “invisible” communication. Steganography means to hide messages existence in a particular medium such as audio, video, image, text communication. In recent steganography systems uses multimedia objects like image, audio, video, etc., as their cover media because people often send digital images over email or may share them through other internet communication application. It is very different from protecting the actual content of a hidden message. Steganography simply means that is not to be alter the any structure of the secret message, but hides it inside a cover-object which is used as medium for transmitting message. After hiding the message, the process cover object and stego-object which helps to carrying hidden information object. So, steganography is used to hiding information and cryptography is used to protecting information are totally different from each another. Due to which the invisibility or hidden factor is so difficult to recover information without any known procedure in steganography. For Detecting information procedure of steganography is known as Steganalysis.

A. *Cryptography and Steganography*

Essence of cryptography method is by upsetting the information content, make it look like random code to achieve the purpose of protecting information content. Information hidden technology is the study of how to hide certain information in another public information, and then to pass hidden information by transferring public information [4]. The technology of information security which is based on cryptography and information security which is based on steganography, is not contradictory and competing with each other but rather complementary. This article is a cryptography and information hiding techniques combined.

B. *RSA Algorithm*

In this paper, we use the RSA public key cryptosystem, which is the first public key algorithm which can be used in digital encryption and digital signature [5]. It has the advantages of easy to understand and easy to operate. The mathematical theory of RSA algorithm is based on a composite number with large number factors is decomposed into two prime numbers is very difficult. In this paper, we use the digital signature system of RSA to authenticate and strengthen security. We should first sign and then encrypt in the realization process [6].

C. Least Significant Bit

Least significant bit (LSB) algorithm used in this paper is a spatial domain steganography in substitution method, the principle is to replace information in the least bit of cover image with confidential information. For 256 gray scale cover image, the gray scale value of each pixel can be used to represent 8-bit binary, taken out a certain bit of all pixels constitute a certain bit plane, for example, the least significant bit of all the pixels constituting the least significant bit plane. The higher the bit plane, the greater the contribution of the gray value, and the lowest bit plane is similar to random noise [7]. As shown in Figure 1, it is the eight bit plane of Lena gray image.

II. LITERATURE SURVEY

Pixel-based algorithms [9]–[11] generate the synthesized image pixel by pixel and use spatial neighborhood comparisons to choose the most similar pixel in a sample texture as the output pixel. Since each output pixel is determined by the already synthesized pixels, any wrongly synthesized pixels during the process influence the rest of the result causing propagation of errors.

Otori and Kuriyama [12], [13] pioneered the work of combining data coding with pixel-based texture synthesis. Secret messages to be concealed are encoded into colored dotted patterns and they are directly painted on a blank image. A pixel-based algorithm coats the rest of the pixels using the pixel-based texture synthesis method, thus camouflaging the existence of dotted patterns. To extract messages the printout

of the stego synthesized texture image is photographed before applying the data-detecting mechanism. The capacity provided by the method of Otori and Kuriyama depends on the number of the dotted patterns. However, their method had a small error rate of the message extraction.

Patch-based algorithms [14], [15] paste patches from a source texture instead of a pixel to synthesize textures. This approach of Cohen et al. and Xu et al. improves the image quality of pixel-based synthetic textures because texture structures inside the patches are maintained. However, since patches are pasted with a small overlapped region during the synthetic process, one needs to make an effort to ensure that the patches agree with their neighbors.

Liang et al. [16] introduced the patch-based sampling strategy and used the feathering approach for the overlapped areas of adjacent patches. Efros and Freeman [17] present a patch stitching approach called "image quilting." For every new patch to be synthesized and stitched, the algorithm first searches the source texture and chooses one candidate patch that satisfies the pre-defined error tolerance with respect

to neighbors along the overlapped region. Next, a dynamic programming technique is adopted to disclose the minimum error path through the overlapped region. This declares an optimal boundary between the chosen candidate patch and the synthesized patch, producing visually plausible patch stitching.

Ni et al. [18] proposed an image reversible data hiding algorithm which can recover the cover image without any distortion from the stego image after the hidden data have been extracted. Histogram shifting is a preferred technique among existing approaches of reversible image data hiding because it can control the modification to pixels, thus limiting the embedding distortion, and it only requires a small size location map, thereby reducing the overhead encountered. The current state-of-the-art for reversible image data hiding is the general framework presented by Li et al. [19].

III. METHODOLOGY

In his section we present the proposed workflow of steganography framework. Fig. 2. Shows the working with its system architecture. Various modules are present in the framework are described below.

1. Input Image
2. Image Quality Selection
3. AES Encryption
4. 2LSB Algorithm
5. Encoded and Encrypted Image

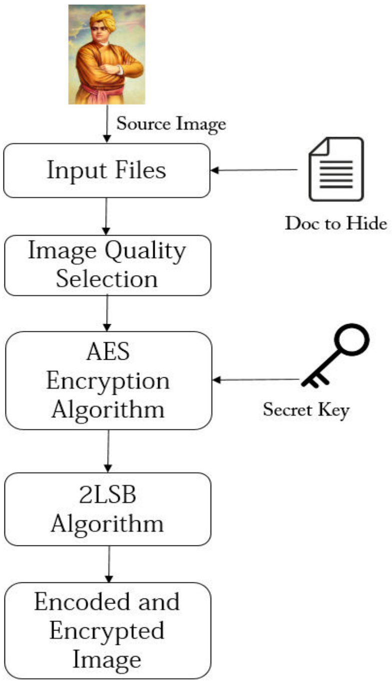

Fig. 2. Propsoed system acrchitecture

A. Input Image

The image is selected to hide the secret information. The information may be in a text file. The length of the files are depends upon the image quality.

B. Image Quality Selection

The output image quality is selected. The more is the image quality the less will be the data can be hidden and wise versa.

C. AES Encryption

AES encryption is used for encryption of the secret data. It provides double layer of security check. If by chance the hacker decodes the text in image file, it will not be able to decode the AES encrypted information.

D. LSB Algorithm

LSB algorithm is sued to hide information on the lower bits of the image. The LSB algorithm is efficient and can hide vast amount of information.

E. Encoded and Encrypted Image

Now, Image is ready to be sent to the third party. The third party if he/she has the secret key to open the AES algorithm then only it can open.

IV. RESULTS

This is section the outcomes are discussed briefly. 2LSB, AES algorithm are for hiding secret information into the image file. Dataset is randomly chosen. There is no need of specific dataset since algorithm work is just to hide secret information.
Fig. 3. Shows the input image.

Fig. 3. Shows the input image

AES and LSB method are applied to encrypt the secret data. By selecting various quality of images thes ecret data can be hidden. Fig. 4. Shows the output of efefct of image quality.

As the image quality is selected as high quality. The secret data can be hidden are very less. But the quality of image remains very high.

If the quality of output image is chosen as mediu qyality, the output image can accommodate only medium content or secret messages. It can be used in webmails.

If the quality of output image is selcted as poor or destroyed quality the information can be stored are enormous. The huge secret messeges can be stored. It can be sued for email messages to fulfill the size restriction of a file.

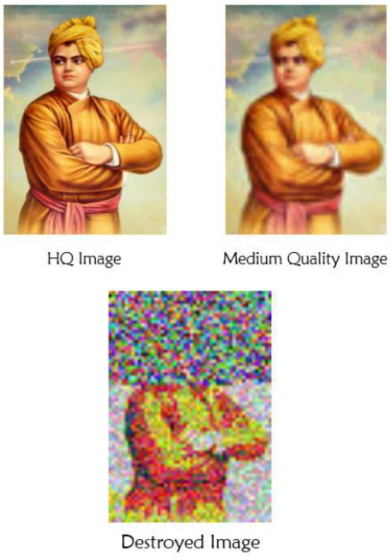

Fig. 4. Image Encoded Quality

V. CONCLUSION

In this paper we propose a novel method image steganography technique in the combination of AES and LSB method. The various image sizes are considered and secret information of different sizes are also considered. .

The framework provides an effective way to select output image toad accommodate the secret information. The receiver needs to have a secret key which will be used to decode the secret message.

REFERENCES

[1] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, vol. 31, no. 2, pp. 26–34, 1998.

[2] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security Privacy, vol. 1, no. 3, pp. 32–44, May/Jun. 2003.

[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hidinga survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[4] Y.-M. Cheng and C.-M. Wang, "A high-capacity steganographic approach for 3D polygonal meshes," Vis. Comput., vol. 22, nos. 9–11, pp. 845–855, 2006.

[5] S.-C. Liu and W.-H. Tsai, "Line-based cubism-like image—A new type of art image and its application to lossless data hiding," IEEE Trans. Inf. Forensics Security, vol. 7, no. 5, pp. 1448–1458, Oct. 2012.

[6] I.-C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," IEEE Trans. Image Process., vol. 23, no. 4, pp. 1779–1790, Apr. 2014.

[7] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," IEEE MultiMedia, vol. 8, no. 4, pp. 22–28, Oct./Dec. 2001.

[8] Y. Guo, G. Zhao, Z. Zhou, and M. Pietikäinen, "Video texture synthesis with multi-frame LBP-TOP and diffeomorphic growth model," IEEE Trans. Image Process., vol. 22, no. 10, pp. 3879–3891, Oct. 2013.

[9] L.-Y. Wei and M. Levoy, "Fast texture synthesis using tree-structured vector quantization," in Proc. 27th Annu. Conf. Comput. Graph. Interact. Techn., 2000, pp. 479–488.

[10] A. A. Efros and T. K. Leung, "Texture synthesis by non-parametric sampling," in Proc. 7th IEEE Int. Conf. Comput. Vis., Sep. 1999, pp. 1033–1038.

[11] C. Han, E. Risser, R. Ramamoorthi, and E. Grinspun, "Multiscale texture synthesis," ACM Trans. Graph., vol. 27, no. 3, 2008, Art. ID 51.

[12] H. Otori and S. Kuriyama, "Data-embeddable texture synthesis," in Proc. 8th Int. Symp. Smart Graph., Kyoto, Japan, 2007, pp. 146–157.

[13] H. Otori and S. Kuriyama, "Texture synthesis for mobile data communications," IEEE Comput. Graph. Appl., vol. 29, no. 6, pp. 74–81, Nov./Dec. 2009.

[14] M. F. Cohen, J. Shade, S. Hiller, and O. Deussen, "Wang tiles for image and texture generation," ACM Trans. Graph., vol. 22, no. 3, pp. 287–294, 2003.

[15] K. Xu et al., "Feature-aligned shape texturing," ACM Trans. Graph., vol. 28, no. 5, 2009, Art. ID 108.

[16] L. Liang, C. Liu, Y.-Q. Xu, B. Guo, and H.-Y. Shum, "Real-time texture synthesis by patch-based sampling," ACM Trans. Graph., vol. 20, no. 3, pp. 127–150, 2001.

[17] A. A. Efros and W. T. Freeman, "Image quilting for texture synthesis and transfer," in Proc. 28th Annu. Conf. Comput. Graph. Interact. Techn., 2001, pp. 341–346.

[18] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[19] X. Li, B. Li, B. Yang, and T. Zeng, "General framework to histogramshifting-based reversible data hiding," IEEE Trans. Image Process., vol. 22, no. 6, pp. 2181–2191, Jun. 2013.

[20] J. L. Rodgers and W. A. Nicewander, "Thirteen ways to look at the correlation coefficient," Amer. Statist., vol. 42, no. 1, pp. 59–66, 1988.

[21] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.

[22] Jharna Chopra, and Sampada K. Satav, " Impact of Encryption Technique Classification Algorithm for preservation of data", published in International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 10, October 2013, at print pages 5398-5402, ISSN: 2319-8753.