Indian J.Sci.Res. 17(2): 350-353, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

A REVIEW ON STEGNOGRAPHIC SYTEM BASED DIGITAL DATA HIDING IN A COLOUR IMAGE USING CRYPTOGRAPHY TECHNIQUE

[1]Ch.Veeranjaneyulu
[2]Assisstant Professor, Department of Electronics and Communication Engineering, CMR College of Engineering And Technology, Hyderabad

Abstract- From thousands of years back our predecessors have invented several ways of passing information in hidden form with other objects like papyrus scroll, cryptex etc. As decades crossed through earth's vein we are getting matured and invented several steganographic systems for message passing. The availability of internet in every corner of the universe forced the user of steganographic systems to invent and implement a better secured algorithm for encryption and decryption of text. Here framework will embed text string into digital colour images and the text that is embedded is perceptually invisible to Human Visual System (HVS). Many text steganographic systems are available that are passing the text with digital media as a form of message digest that can be hacked easily. Here this algorithm supersedes the conventional algorithms. Instead of forming message digest first a 32-bit secret key will be provided by the encrypter and that is applied on the text with a hash function. On the other end if an intruder tries to perform the extraction of the text with a wrong secret key, he will not be succeeded. In the proposed framework the information of Red (R), Green (G) & Blue (B) values of the pixels of the host colour image are retrieved.

Keywords- Steganographic system, Text encryption, Decryption, Secret key, Pixel

I Introduction

For the Data Communication, the security of data transmission is taken into account. The steganographic system attains the high priority for data communication. The key aesthetics of this kind of systems are- quality of encrypted image and security. The digital watermarking and steganography techniques are used for secure data transmission[2]. For vedio authentication also the steganographic systems are used[3] [4] [5]. In the steganographic system, the text messages is passed along with the image by inserting the text directly to LSBs of the image pixel's. This method has some drawbacks, that are-

- The text which is present in the image can be considered as separate part and that can be taken out easily.
- Collaborating the LSBs from the pixels of encrypted image is absolutely easy.

The proposed framework overcomes these drawbacks. Instead of directly inserting the text in colour image, the embedding the text in LSBs of image is done to from the encrypted image. For embedding the text into image, first pseudo text is generated. The pseudo text is generated from 32-bit secret key and HASH function. At the extraction end, the text is extracted with the help of secret key. If the hackers try with an improper key, then the text extracted is not extracted. The pseudo text is used at the embedding side so collaborating of the LSBs also not easy. Without the HASH function and secret key the conversion of pseudo byte stream to original text byte byte stream cannot be done.

II.Embedding The Text

The pseudo text is embedded into the LSBs of host image. That pseudo text is generated from 32-bit key and HASH function[1]. The schematic diagram for embedding the text is shown in figure 1.

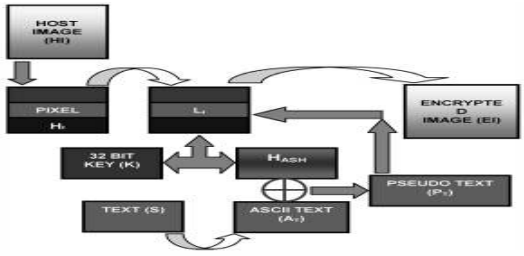

Figure1: Embedding Text

The input is converted to pixel.

A. Pixel: From the image the R,G,B pixel values are taken. The image contains 256*256 pixels of R,G,B. For simplicity i am considering gray scale image that contains only matrix of 256*256. However the entire design will be developed on R,G,B format using 3 matrix information. From the pixel values only LSB bits are taken. This pixel values are converted to binary form.
B. L1: Only the lower bit pixel value are considered. Make the LSBs to zero. From this 8-bit and with the help of key HASH function is generated.

[1]Corresponding Author

C. 32- bit key: This key is in binary form.
D. HASH: The HASH function is the long sequence of bits. For long specified data(key) HASH function will generate 160 bits of data as a HASH value for the applied 32-bit key. For HASH function generation secure hash algorithm is used. Secure HASH Algorith-1 is most widely used of the existing SHA hash function. It produces 160- bit message digest. It differs from previous SHA-0 algorithm by single bit-wise rotation in the message schedule. So that SHA-1 produce the more security than SHA-0. SHA-1 appears to provide greater resistance to attacks, supporting the change increased security.

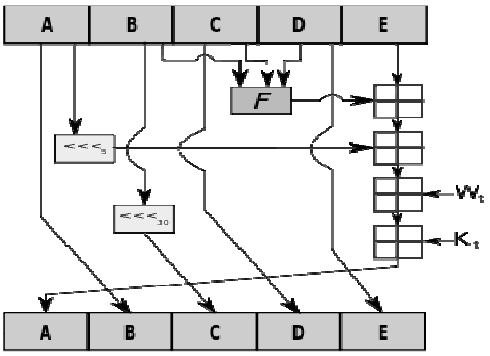

Figure 2: SHA-1

The figure2 shows the one iteration within the SHA-1 compression function. A, B, C, D and E are 32-bit words of the state. *F* is a nonlinear function that varies. $\lll_n$ denotes a left bit rotation by *n* places. *n* varies for each operation. W_t is the expanded message word of round t. K_t is the round constant of round t. $\boxplus$ denotes addition modulo 2^{32}.

The SHA-1 produces 160-bit message digest. Four modulo addition are used, so four round shift operation are done. With the help of expanded message word and constant key the message digest is produced.

E. ASCII text: Text is converted to ASCII form with the help of ASCII table. That ASCII bit is converted to binary form.
F. Pseudo text: The binary converted ASCII text is XORed with HASH function which is generated from SHA-1 algorithm. It produces pseudo text.
G. Encrypted image: The pseudo text is embedded in the zero LSBs, this produces the encrypted image(EI).

III Extracting The Text

The pseudo text is extracted from the image with the help of secret key and HASH function. The text is in the ASCII form. Then that is converted back to text string. The block diagram for extracting the text is shown in figure3.

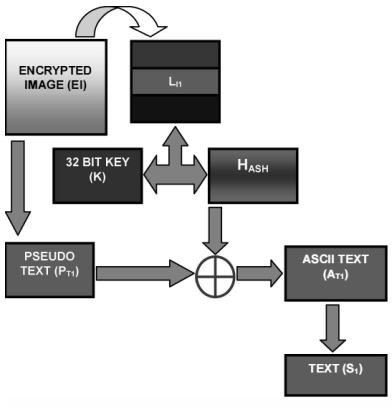

Figure 3: Extracting text

From the encrypted image pseudo text is taken. And make the LSB values zero to form HASH function.

A. Pseudo Text: The pseudo text is taken from encrypted image. The pseudo text is generated by HASH function and ASCII text.
B. L1: Only the lower bit pixel values are considered. Make the LSBs to zero. From this 8-bit and with the help of key HASH function is generated.
C. 32-bit key: This is the secret key. This is in the binary form.
D. HASH: The HASH function is generated from 32-bit and LSBs. It produces the long sequence of binary bits. For the HASH function generation SHA-1 algorithm is used. The HASH function will generate 160 bits data as a HASH value for the applied 32-bit key.
E. ASCII text: ASCII text is produced by XORing pseudo text with HASH. The same HASH is used which is used for encryption side. So it produce the text which is present in the pseudo text. That text is in the ASCII form.
F. Text: The ASCII text which is obtained is converted back to text string. The same text which is embedded in the encryption side is obtained.

IV System Implementation

Implementation is carried out in Labview. Labview implementation of pixel value extraction, shift register, ASCII conversion and pseudo text generation are given below.

A.Pixel value extraction

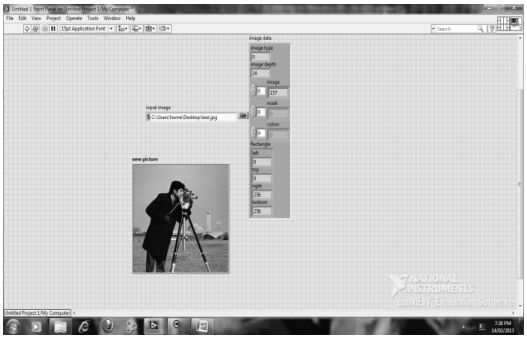

Figure 4: Front panel for pixel value extraction

Figure 4 shows the block diagram of pixel value extraction. The input of this is the camera man image. The JPEG block reads a JPEG file and creates the data necessary to display the file in a picture control. The output of JPEG file is given to the draw flattened block. It draws a 1-, 4-, or 8-bit pixmap or a 24-bit RGB pixmap into a picture.

B.Shift Register

Figure 5 shows the block diagram of shift register. Increment function adds 1 to the input value. And for loop executes its sub diagram n times, where *n* is the value wired to the count **(N)** terminal.

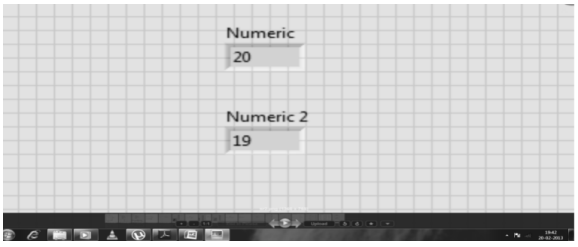

Figure 5: Front panel for shift register

C.ASCII Conversion

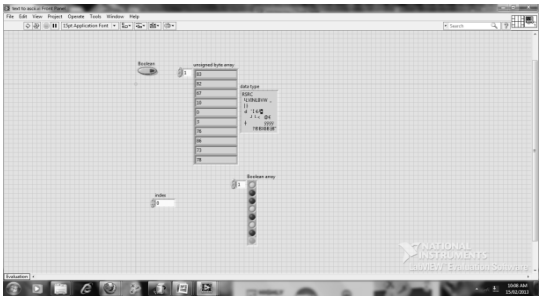

Figure 6: Front panel for ASCII conversion

I. Figure 6 shows the block diagram of ASCII conversion. Read from Text File Function reads a specified number of characters or lines from a byte stream file. String To Byte Array Function converts a string into an array of unsigned bytes. Index Array Function returns the element or sub array of n-dimension array at index**.** Number To Boolean Array Function converts an integer or fixed-point number to a Boolean array.

II. D.Psuedo text generation

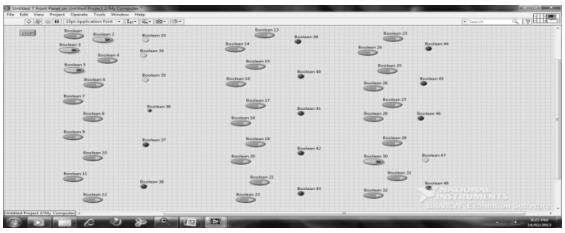

Figure 7: Front panel

III. The block diagram for pseudo text generation is shown in figure 7. XOR gate Computes the logical exclusive or (XOR) of the inputs. Both inputs must be Boolean values, numeric values, or error clusters. One input is HASH function and other input is ACSII converted text.

V Conclusion

Encryption algorithm is able to embed text strings into the colour host images. The pixel values of the image are taken. Shift register is implemented and which will be used to produce the HASH function. The ASCII form of text is converted to Boolean. Pseudo will be generated by XORing the HASH function and text. In the encrypted image the embedded text is entirely invisible. The text extraction framework is blind that guarantees except the secret key nothing is needed to extract the hidden text from encrypted image. The 32-bit secret key and an efficient hash function ensure high security aspects.

References

[1] Soumik Das, Pradosh Bandyopadhyay, Proj Alai Chaudhuri, Dr. Monalisa Banerjee ‘A Secured Key-based Digital Text Passing System through Color Image Pixels’ published in IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012. ISBN: 978-81-909042-2-3 ©2012. Vol 320-325.

[2] Dr. Neil F. Johnson ‘digital watermarking and steganography’ published in 8th International Information Hiding Conference (IH2006) in Old Town Alexandria, USA - held 10-12 July, 2006 .Vol 476-483

[3] Soumik Das, Pradosh Bandyopadhyay, Shauvik Paul, Atal Chaudhuri and Monalisa Banerjee. Article: An Invisible Color Watermarking Framework for Uncompressed Video Authentication. International Journal of Computer Applications 1(11):22–28, February 2010. Published By Foundation of Computer Science.

[4] PradoshBandyopadhyay, Soumik Das, Shauvik Paul, Prof. AtalChaudhuri, Dr.Monalisa Banerjee, "A Dynamic Watermarking Scheme for Color Image Authentication"- Published in Proceedings of IEEE International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom-2009), Kerala, India, October 2009. Uploaded in IEEE Xplore, (ISBN: 978-0-7695-3845-7).

[5] Soumik Das, PradoshBandyopadhyay, Prof. Alai Chaudhuri, Dr.Monalisa Banerjee, "Uncompressed Video Authentication Through AChip Based Watermarking Scheme"- Published in 2nd InternationalConference on Emerging Applications of Information Technology(EAIT-2011), Computer Society of India, India, February, 2011. (ISBN: 978-0-7695-4329-1).

[6] http://www.ipcsit.com/vol21/19-ICSIA2011-A1012.pdf

[7] http://www.rroij.com/open-access/fpga-implementation-of-vigenere-ciphermethod-based-on-colour-image-steganography.php?aid=42972

[8] http://www.ijirae.com/volumes/Vol2/iss3/12.MREC10098.pdf

[9] http://www.ijarcce.com/upload/2016/may16/IJARCCE%202.pdf

[10] http://docsdrive.com/pdfs/ansinet/jas/0000/40289-40289.pdf

[11] https://arxiv.org/ftp/arxiv/papers/1112/1112.2809.pdf

[12] https://www.ijedr.org/papers/IJEDR1701003.pdf

[13] http://publications.drdo.gov.in/ojs/index.php/dsj/article/viewFile/1436/601

[14] International Journal of Recent Research and Review, Vol. VII, Issue 2, June 2014 ISSN 2277 – 8322