www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Volume-7, Issue-4, July-August 2017

International Journal of Engineering and Management Research

Page Number: 61-64

Increased Embedding Rate by Reversing the Order of Data Hiding and Encryption

Nitin Kumar Agrawal[1], Nikhil Kumar[2], Dr. Sanjeev Kumar[3]

[1,2]M.Tech Student (Signal Processing), Electronics and Communication Engineering, Ambedkar Institute of Advanced Communication Technologies & Research, Delhi, INDIA

[3]Assistant Professor, Electronics and Communication Engineering, Ambedkar Institute of Advanced Communication Technologies & Research, Delhi, INDIA

ABSTRACT

In this paper we are hiding data into two different ways one is data hiding before encryption and other is data hiding after encryption. We are hiding the data into the image by using data hiding key firstly before encryption and then hiding the data into the image after encryption. At the receiver side the original image can be recovered by providing the same key for decryption as done in encryption in order to get the hidden data. Comparison of two retrieved image is done by the PSNR. The results of data hiding after the encryption are much better than that of data hiding into the image before encryption. The embedding rate is also increased by 2.23% using data hiding after encryption than data hiding before encryption.

Keywords-- Data Hiding, Data Embedding, Data Extraction, Image Extraction

I. INTRODUCTION

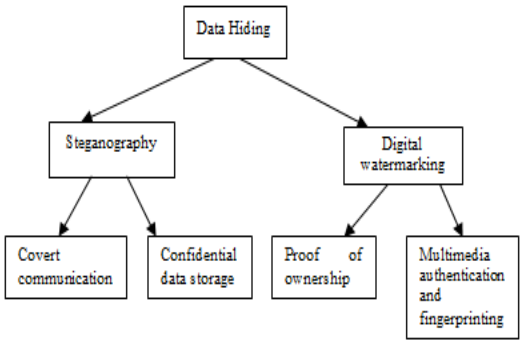
Data hiding is a process of concealing some additional information into a digital signal (it can be video, audio and image) within the signal itself. We need it for safety and privacy of user's data. In this technique the additional data is inserted into a small chunk (portion) of image so that actual image and additional data can be obtained at the receiver. Data hiding and Encryption are the two processes have been utilized in this paper. Where data hiding is a technique of inserting additional data into the original image. By doing some alteration in the pixel values of original image. Encryption is used to transform the plain image into cipher image which conceal the real meaning of the image or in other word it cannot be readable only possible if it is decoded at other side. Some part of the actual image is used to carry the additional inserted data or additional message and image is encoded for privacy protection. The transmitter encrypts the image for secrecy and also hides the data into the image so that no one knew what the image is and what data it is containing. The authorized recipient can only retrieve the exact data and image with some distortion. Data hiding and encryption all we are doing for the confidential communication between the two authorized users. It is greatly used in the field of military where information is highly confidential also used in medical reports and content owner's identification etc.

A large number of explorations have been done on reversible data hiding from [1]-[5]. J. Tian [1] The data hiding is done by increasing the difference between the adjacent pixel values to embedded data. In [2] the data is inserted in the LSB of pixel. [3] Shifting of histogram bins of the image to insert the additional message bits. In [4]-[5] more efficient way of inserting data into the image by reversible watermarking and interpolation in the pixel value. In [6] compressing the LSB of the pixel value is done for the insertion of data and also obtain the data and image at the receiver without any error by exploiting the spatial correlation for small payload. [7] In this after extraction of image and data the smoothness of each block of pixel is examine by pixel correlation of neighboring block. In [8] consider the pseudo random bits of sequence r the input image is encoded by X-OR operation with that sequence. The segment of image into block which is non overlapping and of fixed size $s \times s$ further each block is partitioned into sets namely S_0 and S_1 where one additional message bit is carried by each block. In all the above techniques after data obtain at the recipient side the image is retrieve with the help of spatial correlation.

Methods of Data hiding

Watermarking: If there is an image of an owner then watermarking is the only technique which can provide the authentication and identity of the owner. The verification of owner of an image is inserted into the image. These identification marks are visible.

Steganography: It is also a method of concealing the additional data into the image. It is not visible. The pixel values are altered in such a manner that the additional message which is inserted into the image is seen only by the intended receiver.



Encryption and Decryption

- The process of encoding messages or information by using a random key in such a way that only intended recipient can read it is called as encryption.
- Encoding is very helpful in security of data.
- A plain text is encoded using various algorithms, generating cipher text that can only be read if decoded.
- It conceals the real meaning and cannot be readable image or text.
- By the same key the message at the receiver can be decode.

A. Image encryption

Image can be encoded by generating a pseudo random bits and providing an X-OR operation with each pixel bit of actual image. In [6] the encryption of original image is done by converting it into cipher image. Each bit of an encryption key is performing an X-OR operation with each bit of pixel of the cover image. Each pixel with gray value lies in between [0,255] and it is denoted by 8 bits. Let us consider an original image namely A having w $\times h$ as size of image. Where the value assigning to each pixel of $A_{i,j}$ at points (i,j). The 8 different bits can be written as$A_{i,j}^{(0)}, A_{i,j}^{(1)} \dots\dots\dots\dots, A_{i,j}^{(7)}$.

$$A_{i,j}^{(k)} = \lfloor A_{i,j}^{(0)}/2^k \rfloor \bmod 2 \qquad 0 \le k \le 7 \quad (1)$$

Any pseudo random sequence of size $w \times h \times 8$ are generated which can be used as encryption key.

$$r = \left\{ r_{i,j}^{(k)} \middle| r_{i,j}^{(k)} \in \{0,1\} \right\}_{k=0}^{7} \quad 0 \le i \le w\text{-}1,\ 0 \le j \le h\text{-}1 \quad (2)$$

The above equation performs the X-OR operation with the actual image pixel bits and converts it into cipher image i.e.

$$A_{i,j}^{\prime(k)} = A_{i,j}^{(k)} \oplus r_{i,j}^{(k)}$$

Where $A_{i,j}^{\prime(k)}$ will be the encrypted image.

B. Data embedding

Now the encoded image in [6] can be used to transfer additional message signal by just modify some portion of the encoded image. The encoded image is partitioned in to nonoverlapping block and every individual block having the size of s×s.

Each chunk (block) is further sectioned into two set S_0 andS_1. Each block carry one additional bit where set S_0 carry bit '0' while set S_1 carry bit '1'. If bit '0' to be inserted in any block then 3 LSB of set S_0 flip and for bit '1' 3 LSB of set S_1 flip. Each block of image is denoted by $H^{m,n}$ which are having the position at (m,n).

$H_{u,v}^{\prime m,n} = \overline{H_{u,v}^{\prime m,n}}$, (u,v) ∈ S_0, k = 0,1,2

$H_{u,v}^{\prime m,n} = \overline{H_{u,v}^{\prime m,n}}$, (u,v) ∈ S_1, k = 0,1,2

Embedded Bit	Set	Bits Flip
0	S_0	3 LSB
1	S_1	3 LSB

Now each block is embedded with one additional bit of message signal. The original image is first encrypted and embedded with message signal.

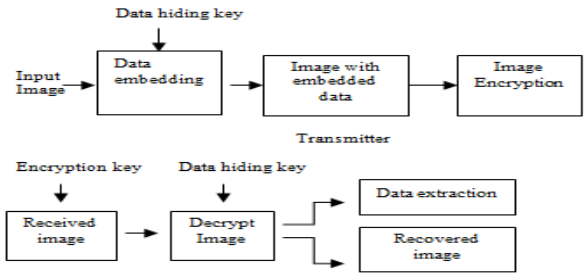
C. Data extraction and image recovery

In [6] at the receiver side the encrypted image is first decrypt by applying the same key r which is applied at the transmitter side to encrypt. The X-OR operation have this special property that if we apply the X-OR operation on any signal twice it will become the same as it was original the same way as if we invert anything twice then it will be on its original position.

- The original five most significant bits (MSB) are retrieved correctly.
- If 0 is inserted in the pixel's block then the pixel belongs to S_0 , or 1 is inserted in the pixel's block then the pixel belongs to S_1.
- The three decoded LSB must be same as the original LSB in order to get the actual image as it was sent at the transmitter without any error.

Data hiding directly into the image and then encode the image is sometime provide inefficient result than data hiding into the encoded image. So if we reverse the order of encryption at the transmitter side i.e. first encryption and then data hiding this will lead to increased payload.

Fig 1(a). Structure for data hiding before encryption as follow: - At the transmitter side data hiding key is used to hide the data into the actual image. The Data inserting process is done by shifting some of the LSB pixel. After data embedding into the actual image the image is encoded by providing the encryption key. At the recipient side the image is first decoded and data hiding key is used to extract the data as well as the retrieve image.



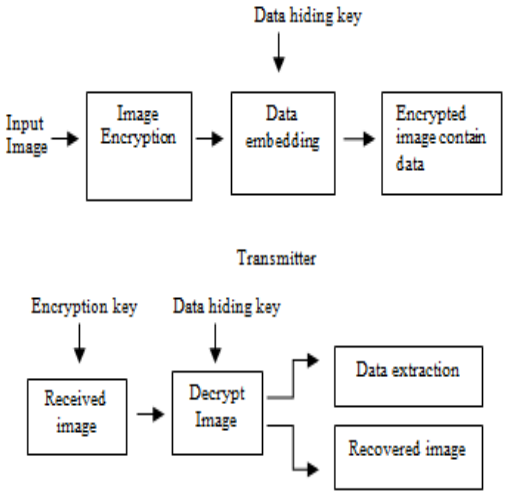
Receiver
Fig 1(a)

Algorithm Used
Transmitter:
1. Input image
2. Data hiding key to hide the data
3. Image encryption

Receiver:
1. Decrypt image
2. Data hiding key for data and image extraction
3. Data recovery
4. Image recovery.

Disadvantage:
1. Error arises while obtaining the data and image restoration process at the recipient end.

Now Fig 1(b) Structure for data hiding after encryption as follow: - The input image is provided by the owner that is first encoded by using the encryption key and also providing the data hiding key for the inserting of the additional message into the image. The encoded image containing the data is transmitted to the recipient now this image is first decode by using the same key as at the transmitter which will obtain the additional message also the retrieved image.



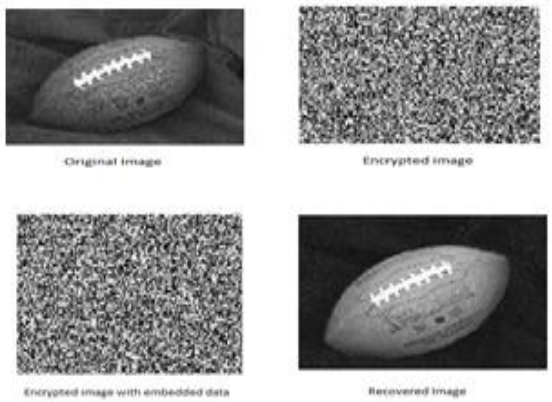
Receiver
Fig 1(b)

Algorithm Used
Transmitter:
1. Input image
2. Image encryption
3. Data hiding key to hide the data

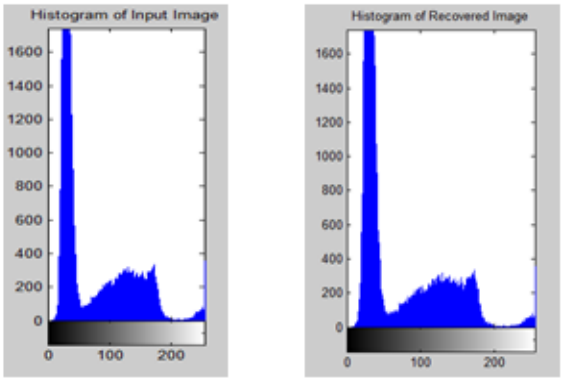
Receiver:
1. Decrypt image
2. Data hiding key for data and image extraction
3. Data recovery
4. Image recovery.

Advantage:
- PSNRs of decrypted image containing the embedded data are significantly improved.
- Range of embedding rates is greatly enlarged.

II. EXPERIMENTAL RESULTS



This experiment has been done by taking an image of football of size 512 × 512. This image is considered as the original image. All the operations i.e. image encryption,data hiding,image decryption finally data and image recovery done on this image. Firstly the image is converted in to the encrypted image by performing an X-OR operation with any random sequence of bits. This sequences is of 8 bit which perform bit wise X-OR operation with every bit of original image. Encrypted image is divided into blocks and each block carry one message bit. Each block size having the length 32. Thus, 256 bits can be embedded in to the original image. As if we increase the size of the block then more bits can be added into the image but the recovery of image and data extraction obtained with an error. This happen because of spatial correlation for the small block size such that the extraction of image and data can be easily obtained. As the embedding rate increases the recovery becomes difficult contain error.



The output can also be examine with the help of histogram of the input image compared with the histogram of the image after extraction of data but clear result can be seen in the PSNR table 1.

Table 1

S.NO.	PSNR (db) Before encryption	PSNR (db) After encryption	Recovered rate (bpp)
1	55	55.3	0.2
2	52	52.8	0.3

3	49.2	50	0.4
4	47.1	48	0.5
5	44.8	45.8	0.6

The PSNR of the recovered image is obtained and it is varying as the number of bits increase to embed in the original image. The maximum deviation can be seen in the table when the data embedding rate is 0.6 bits per pixel. The PSNR for before encryption technique is 44.8 and which is increased to 45.8 for the technique data hiding after encryption. This shows that data embedding rate is increased approximately 2.23% and recovery can also be done easily for small payloads. But as if we increase the size of the block to carry additional information in that case the embedding will increase but the recovery of image and data will be contaminated with error which means exact image and data cannot be recovered.

III. CONCLUSION

The main aim of this paper is to compare the results of two data hiding techniques. More attention is given to the reversible data hiding because of the privacy required by the content owner and encryption is also used which conceal the real meaning of the image. A lot of work has been done on reversible data hiding [1] to [5]. But in this paper data hiding after encryption which consist of image encryption, data embedding by using the data hiding key and data extraction and image can be recovered by using the same key at the transmitter [6]-[8]. This method does not improve the image quality but by applying the proposed method the payload can be increase which means more data can be transmitted without an error i.e. embedding rate increases.

REFRENCES

[1] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, 2003.
[2] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized- LSB data embedding, " *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253–266, 2005.
[3] Z. Ni, Y. Q. Shi, N. Ansari, andW. Su, "Reversible data hiding," *IEEE* Trans. Circuits Syst. Video Technol., vol. 16, no. 8, pp. 354–362, 2006.
[4] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, 2007.
[5] W. Hong and T. S. Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism," J. Vis. Commun. Image Represent., vol. 22, no. 2, pp. 131–140, 2011.
[6] X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.
[7] W. Hong, T. Chen, and H.Wu, "An improved reversible data hiding in Encrypted images using side match," *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 199–202, Apr. 2012.J.
[8] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.