ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

DYNAMIC BLOCK BASED ENCODING SCHEME FOR DATA HIDING USING IMAGE FEATURES

B.Chitradevi[1], Dr.S.Manikandan[2]
[1]Research Scholar, Research and Development Centre, Periyar University, Salem
[2]Head, Department of Computer Science and Engineering, Sri Ram Engineering College, Chennai

Abstract

One of the problems focused more in recent days is data hiding and there are some methods have been discussed in previous days. Since, the accuracy of the existing approaches is very less this paper motivated provide an efficient approach for data hiding using image information. A dynamic block selection technique is discussed. In this scheme, the first 3×3 block plays the vital role which contains the Meta information about the encoding scheme. The method stores different information regarding the encoding scheme in the first block. The diagonal element includes the information about the coding scheme. First, from the first block, the method computes the number of blocks to be used and store in the first index. Then the method identifies the minimum value from the first block and selects the number of blocks based on the power function. According to the result of the power service, some blocks will be chosen according to the length of the message to be encoded. The message will be encrypted in the diagonal elements and will be decoded in the same procedure at the receiving side.

Index Terms

Information Security, Data Hiding, Data Encoding, Steganography, Reversible encoding, Dynamic Block Selection

Introduction

Development of computer technology and widespread use of internet have driven this world into fast-changing digital place. With digitization of multimedia contents, everybody can access multimedia contents more easily than in analog age. Even if digitization of multimedia contents provides more opportunities to media contents, it also provide easy access paths to copy and distribution of digital contents, because of characteristics of the digital data, represented by 0 and 1. As the copy and distribution of digital contents are widely conducted illegally in internet environment, the copyright holders began to pay attention to copyright protection technologies. Off the technologies that can protect copyright of digital contents, data hiding technology has received keen interests from research communities Data hiding process is to be such that the modifications of the media are imperceptible. F or images same as digital watermarking, is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners. In digital watermarking, it describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has this means that the modifications of the pixel values have to be invisible. The signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in copy. Reversible data embedding, which is also called lossless data embedding, embeds invisible data (which is called a payload) into a digital image in a reversible fashion. As a basic requirement, the quality degradation on the image after data embedding should be low. An intriguing feature of reversible data embedding is the reversibility,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

that is, one can remove the embedded data to restore the original image. From the information hiding point of view, reversible data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original, pristine state.

Related Works

The motivation of reversible data embedding is distortion-free data embedding [1]. Though imperceptible, embedding some data will inevitably change the original content. Even a very slight change in pixel values may not be desirable, especially in sensitive imagery, such as military data and medical data. In such a scenario, every bit of information is important. Any change will affect the intelligence of the image, and the access to the original, raw data is always required.

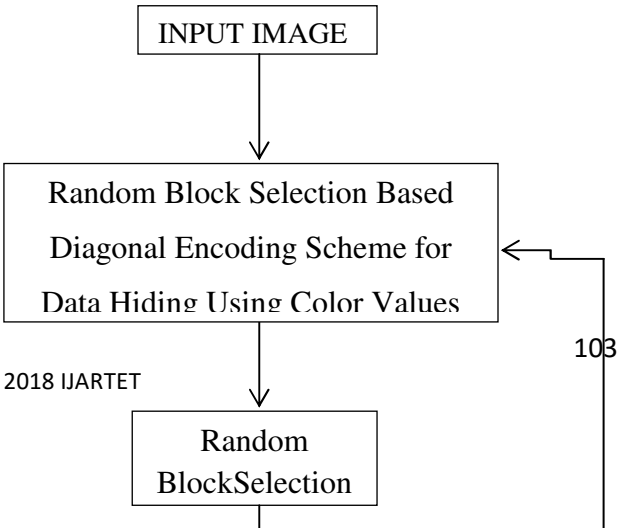
Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption [1], propose a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. Experiments show that this novel method can embed more than 10 times as large payloads for the same image quality as the previous methods, such as for PSNR=40 dB.

Reversible Data Hiding in Encrypted Image [2], proposes a novel reversible data hiding scheme for encrypted image. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. A Reversible Data Hiding Method for Encrypted Images [4], original work partitions an encrypted image into blocks, and each block carries one bit by flipping three LSBs of a set of pre-defined pixels.

The data extraction and image recovery can be achieved by examining the block smoothness. Zhang's work did not fully exploit the pixels in calculating the smoothness of each block and did not consider the pixel correlations in the border of neighboring blocks. Secure and Authenticated Reversible Data Hiding in Encrypted Images [6], proposes a Secure and authenticated discrete reversible data hiding in cipher images deals with security and authentication. Joint reversible data hiding and image encryption, Image encryption process is jointed with reversible data hiding in this paper, where the data to be hided are modulated by different secret keys selected for encryption.

Dynamic Block Selection Approach Based Reversible Diagonal Encoding Scheme:

Thedynamic block selection approach reads the secret input image and computes the number of blocks to be used. Then the method identifies the minimum number and calculates the power of selected number to determine the block. Based on the block selection, the input string is encoded in the diagonal elements andthe same is reversed to perform the decoding process. The entire process has been split into the number of stages namely.



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

The Figure 1, shows the structure of diagonal encoding scheme and shows the functional components in detail. [7] proposed a principle in which the division is the urgent stage in iris acknowledgment. We have utilized the worldwide limit an incentive for division. In the above calculation we have not considered the eyelid and eyelashes relics, which corrupt the execution of iris acknowledgment framework. The framework gives sufficient execution likewise the outcomes are attractive. Assist advancement of this technique is under way and the outcomes will be accounted for sooner rather than later. Based on the reasonable peculiarity of the iris designs we can anticipate that iris acknowledgment framework will turn into the main innovation in personality verification.In this paper, iris acknowledgment calculation is depicted. As innovation advances and data and scholarly properties are needed by numerous unapproved work force. Therefore numerous associations have being scanning routes for more secure confirmation strategies for the client get to. The framework steps are catching iris designs; deciding the area of iris limits; changing over the iris limit to the binarized picture; The framework has been actualized and tried utilizing dataset of number of tests of iris information with various complexity quality.

3.2 Dynamic Block Selection:

The method first reads the input image and split the entire image into a number of sub-sampling images. Also from the data message given the number of blocks required is identified. From the first block of the picture, the method determines the minimum intensity value. Then the method computes the number of power blocks based on the value determined. Based on the calculated power blocks, the blocks to be used to perform encoding are selected. The selected blocks are used to perform encryption

Algorithm
Input: Image Img, Message Ms
Output: Selected Blocks.
Start
Read Input Image Img.
Initialize Box size Bs.
Generate subsampling image.
Image set Is = $\int_{i=1}^{size(Img)} Crop(Img, (i \times Bs))$
Read first block B.
Identify the minimum intensity value.
Mv = $\int_{i=1}^{Bs} Min(B, Mv)$
Nb = Compute size of message Ms.
Compute the blocks to be used.
Block set Bls = $\int_{i=1}^{Nb} Mv^i$
Stop.

The above-presented algorithm selects the blocks to be used to perform encoding the original message.

3.3 Encrypting 1-Bin MPE2 Algorithm

To embed secret messages S, let CI be an 8-bit gray scale image with size M × N and (i, j)

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

be the pixel located on row i and column j in image CI, $1 \leq i \leq M$, $1 \leq j \leq N$. SI is the stage image, and the size is the same as CI. Note how the cover image is only used to initialize the first row and first column of the stage image. The embedding procedure of our algorithm involves calculating the prediction errors from the neighborhood of a given pixel and then embedding the message bits in the modified prediction errors. The detailed embedding steps are as follows:

Embedding Procedure ( )
{
Input: $Ann - bitsecretmessageSand$
$8 - bitsM \times Ngrayscalecoverimage CI.$
Output: $AM \times NstageimageSI, endof$
$embeddingpositionL, andadatastructure$
$Ocontainingtheoverheadinformation.$

The assumption in this algorithm is that the used predictors are 3x3 and causal. Thus, the scanning in the embedding procedure excludes the first column and first row in the image, so, these pixels are not used for embedding. The algorithm can be easily modified to accommodate for larger and non-causal predictors. Note that the overhead data structure O is used to save the locations of the pixels at which embedding may cause overflow or underflow. Because no changes are allowed to the prediction errors if the pixel value after modified is overflow or underflow case in order make this approach reversible. Fortunately, the size of overhead data structure O is often zero or negligibly small for most original images since the overflow/underflow problem rarely occurs. Also, the last embedding location in the embedding level is saved in the overhead data structure O.

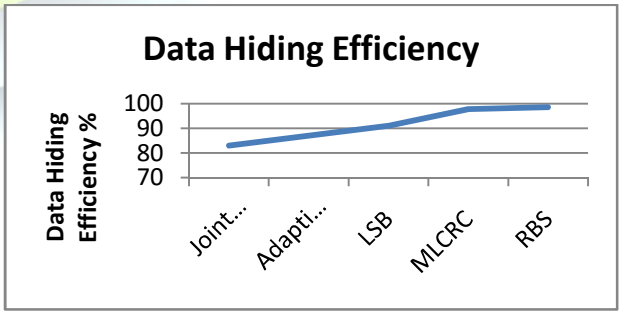
3.4 Extraction Procedure

The Extraction Procedure of the 1-Bin MPE2 Algorithm Using the same scan order sequence in the embedding process, we predict the pixel values again using the same predictors, and calculate the prediction errors PE1 and PE2 at each pixel in the stage image SI. Then we can restore the original image and the secret data.

Image_Reconstruction( ) {
Input: $AM\ X\ NstageimageSIanda$
$datastructure$
$Ocontainingtheoverheadinformation.$
Output: $Ann - bitsecretmessageSand$
$8 - bitM \times Ngray$
$- scalerecoveredimageOI.$

Results and Discussion

The proposed dynamic block selection technique has been implemented and produces efficient results on data hiding. The proposed method has been applied using Matlab. The performance of the method has been tested with various simulation setups and has been tested with different input pattern of data. The method has produced practical results in data encoding and decoding phases. Also, the process has produced the practical result in tamper resistance and has produced less time complexity.



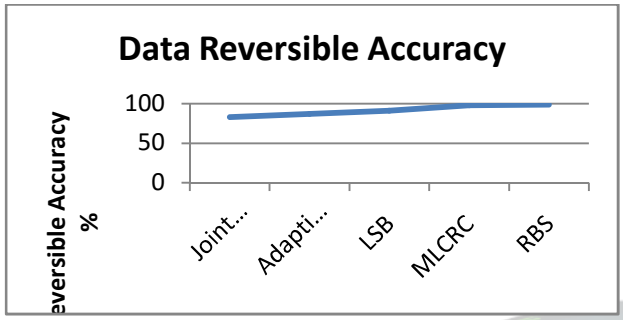
Graph 1: Comparison of data hiding efficiency

The Graph 1 shows the comparison of data cache efficiency produced by different

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

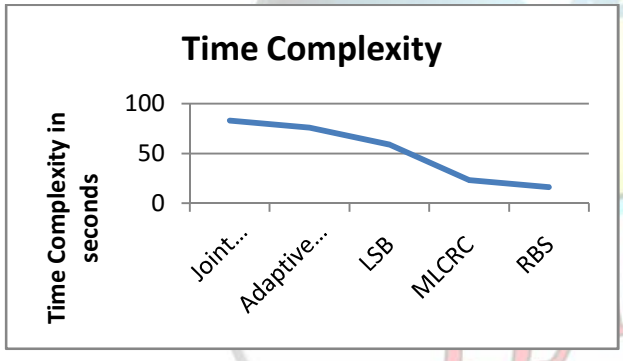
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

methods and it shows clearly that the proposed method has provided more energy than other methods.



Graph 2: Comparison of reversible data accuracy

The Graph 2 shows the comparison result of reversible data accuracy of different methods and it shows clearly that the proposed method has produced more data reversible accuracy than other methods.



Graph 3: Comparison of Time complexity

The Graph 3 shows the comparison of time complexity produced by different methods and it shows clearly that the proposed method has produced less time complexity than other methods.

Conclusion

In this paper, a dynamic block selection technique has been discussed. The method first computes the size of an image and based on that the method calculates the number of blocks to be used. Then the method computed the minimum value of the first block and based on the power function some blocks is identified. The method calculates the right diagonal average to be store at the bottom. The first index of the each block is used to store the value. At the decoding phase, the presence of the secret message is identified by computing the average and presence in the diagonal element. The method has been implemented and tested for its efficiency. The method has produced practical results in all the factors of data hiding and reduced the time complexity also.

References

[1] Ma, K.; Weiming Zhang; Xianfeng Zhao; Nenghai Yu; Fenghua Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" *IEEE Transactions onInformation Forensics and Security,* , vol.8, no.3, pp.553,562, March 2013.

[2] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image",*IEEE Transactions onInformation Forensics and Security,* vol.7, no.2, pp.826,832, April 2012.

[3] Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image," *IEEE Signal Processing Letters,* vol.18, no.4, pp.255-258, April 2011.

[4] W. Puech, M. Chaumont and O. Strauss, "A Reversible Data Hiding Method for Encrypted Images", *SPIE Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents*, San Jose, CA, USA, July 2008.

[5] Manikandan R, UmaM, and MahalakshmiPreethiS M, "Reversible Data Hiding for Encrypted Image" *Journal of Computer Applications*,Volume-5, Issue EICA2012-1, pp. 104-110, February 10, 2012.

[6] V.Khanaa, and Krishna Mohanta, "Secure and Authenticated Reversible Data Hiding in Encrypted Images", *International Journal of Engineering and Computer Science*, Vol. 2, Issue 3, pp. 558-568, March 2013.

[7] Christo Ananth,"Iris Recognition Using Active Contours",International Journal of

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

Advanced Research in Innovative Discoveries in Engineering and Applications [IJARIDEA], Volume 2,Issue 1,February 2017,pp:27-32.

[8] Zhicheng Ni; Yun-Qing Shi; Ansari, N.; Wei Su, "Reversible data hiding," *IEEE Transactions onCircuits and Systems for Video Technology,* vol.16, no.3, pp.354,362, March 2006.

[9] Wien Hong, Tung-Shou Chen, Chih-Wei Shiu , " Reversible data hiding for high quality images using modification of prediction errors", *Journal of Systems and Software*, Volume 82, Issue 11, Pages 1833-1842, November 2009.