International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 9
ISSN: 2454-4248
59 – 62

Study of Reversible Scheme for Data Hiding

Mahip M. Bartere*, Dr. Hemant R. Deshmukh**
*(Sant Gadge Baba Amravati University, Amravati, Maharashtra
Email: *mahip.bartere@gmail.com*)
** (Professor, Dr. Rajendra Gode Institute of Technology & Research Amravati, Maharashtra)

Abstract: Web is the prominent correspondence media now a days yet message exchange over the web is confronting a few issue, for example, copyright control, information security, information, confirmation and so forth. Information stowing away assumes a critical part in information security. It is a procedure in which mystery information or data is put away or covered up into cover media. Thus many explores are advancing on the field like web security, steganography, and cryptography. At the point when exchange the safe or private information over a shaky channel it is expected to encode cover or unique information and after that insert the protected information into that unique or, on the other hand cover picture.

Keywords — *Image encryption, image recovery, reversible data hiding*

*****

I. INTRODUCTION

Steganography is the art and science of secret communication between sender and receiver. This is accomplished through hiding one type of information in other type of information, thus hiding the existence of the communicated information. Steganography, which literally means “covered writing” in Greek, is the process of hiding data under a cover medium, such as image to establish secret communication between trusting parties. The main objective of data hiding is to communicate secretly in such a way that the true message which is embedded in cover image or media is not visible to the observer. That is unwanted parties should not be able to distinguish in any sense between cover-image and stego-image (modified cover-image that contains secret image). Thus the stego image should not deviate much from the original cover image.

Now a day the data security and data integrity are the two challenging areas for research. There are so many research is progressing on the field like internet security, steganography, cryptography. Sometimes we found certain distortion in images used in military, medical science which is un-acceptable. Hence for data hiding we have a technique using which we can extract data correctly and after that original cover content can be perfectly recovered. This technique is known as reversible data hiding. This technique is also called as lossless, distortion free and reversible data hiding technique which enables the exact recovery of the original signal with the extraction of the embedded information. And this exact recovery with lossless data is nothing but the reversible data hiding. Reversible data hiding is a technique that is mainly used for the authentication of data like images, videos, electronic documents etc.

The term "reversible data hiding" means getting the exact recovery of the data after performing the process like encryption-decryption and data hiding. Now the question is; what is mean by "separable reversible data hiding technique"? The word separable means it separates two major activities in this scheme. These two activities are getting the exact recovery of the secure hidden image and exact recovery of cover image. By using this scheme image is hidden into a cover image or media. At the receiver side it must be able to extract the hidden image. In some high-precision applications such as medical, military, it is highly desired that the original image should be perfectly recovered after data extraction.

As the technology has increased day by day the usage of multimedia, web documents and images has also increases on the network. Large amount of images are transferred on the internet every day, so it’s necessary to provide security to these images from the hackers. It may happen that the hackers may capture the images, view the important contents and after viewing the contents they can modify the images and send it to destination. So the original image contents will be modified and the receiver can be totally unaware from this fact. Due to this, a small amount of distortion has occurred. Such distortion is not acceptable in some applications, such as medical imaging or in military images etc. From this point of view a data hiding technique, which is referred to as reversible, invertible, lossless or distortion-free, has been developed in recent years.

II. LITERATUER SURVEY

In 1999 Yeuan Kuen Lee and Ling Hwei Chen proposed a An adaptive steganographic model based on min error LSB placement the model [1] is used for reduce embedding error and provide higher embedding capacity. But this model is useful only for gray scale images.

In 2000 Y. K Lee, L. H Chen proposed a High capacity image steganogrphic model [2] this model is used for

 ISSN: 2454-4248
59 – 62

to maximize the embedding capacity while maintaining image fidelity. This will work only on gray scale images.

In 2001 Giuseppe Atenies, Carlo Blundob, Alfredo De Santisb, Douglas R.[3] proposed a extended capabilities of visual cryptography to share the secret information but these shares are meaningful shares but this have poor display quality.

In 2003 Chang Chou Lin, Wen Hsiang Tsai proposed a Visual cryptography for gray-level images by dithering techniques [4].The proposed system useful for visual encryption and decryption for gray scale images. It cannot be done on color visual information.

In 2004 Tung-Hsiang Liu and Long Wen Chang, proposed data hiding technique for binary images. The proposed method embeds secure data at the edge portion of host binary image. Binary images consist of only two colors therefore changing any pixels in this image could be easily detected by human eyes [5]. We find the best changeable pixels in a block by changing distance matrix dynamically and compute its changeable score by weighting mechanism. The proposed method uses the pseudo random number generator based on Rabin Public Key Cryptography System to embed secret data into a binary image. According to the pseudo random number generator, we can distribute secret data into the binary image to make binary image quality better and get high security.

In 2005 H. C. Wu, N. I. Wu, C. S. Tsai and M. S. Hwang proposed Novel stenographic method based on LSB Replacement and Pixel Value Differencing (PVD) methods to improve the capacity of the hidden secret data and to provide an imperceptible stego-image quality. First, a different value from two consecutive pixels by utilizing the PVD method is obtained [6]. A large difference value can be located on an edged area smooth area and the small one can located on smooth areas. Because the range width is variable, and the area in which the secret data is concealed by LSB or PVD method are hard to guess, the security level is the same as that of a single using the PVD method of the proposed method [7]. From the experimental results, compared with the PVD method being used alone, the proposed method can hide much larger information and maintains a good visual quality of stego-image.

In 2006 Z. Ni, Y. Q. Shi, N. Ansari and W. Su proposed data hiding technique for binary images. The proposed method embeds secure data at the edge portion of host binary image. Binary images consist of only two colors therefore changing any pixels in this image could be easily detected by human eyes [7]. We find the best changeable pixels in a block by changing distance matrix dynamically and compute its changeable score by weighting mechanism. The proposed method uses the pseudo random number generator based on Rabin Public Key Cryptography System to embed secret data into a binary image.

In 2007 Ching Nung Yang and Tse shih Chen proposed an Extended Visual Secret Sharing Schemes: Improving the Shadow Image Quality in this paper they present a new EVSS scheme by using gray and white sub pixel to represent a secret pixel and then gives a clearer shadow images. But it displays low quality images [8].

In 2008 Beenish Mehboob and Rashid Aziz Faruqui. This paper discussed the art and science of Steganography in general proposed Novel technique to hide data in a colorful image using LSB. Many techniques are used to hide data in various formats in steganography [9]. Least Significant Bit or its variants are normally used to hide data in a digital image. The idea of playing with 0's and 1's seem quite simple but a slight change in value may transform an image completely. The other bits may be used but it is highly likely that image would be distorted.

In 2009 Amanpreet Kaur, Renu Dhir, and Geeta Sikka proposed Image Steganography Based on First Component Alteration Technique. In this paper, new steganography scheme introduced spatial domain technique [10]. Using first component alteration technique, hide secret data in cover-image. Techniques used so far focuses only on the two or four bits of a pixel in an image (at most five bits at the edge of an image.) which results less peak to signal noise ratio and high root mean square error [10]. The future work is to modify given scheme to improve image quality by increasing PSNR value and lowering MSE value.

In 2010 M.B. Ould Medeni proposed a novel steganographic method for hiding information within the spatial domain of the gray scale image. The proposed approach works by dividing the cover into blocks of equal sizes and then embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel. The experimental results have shown that the proposed method not only has an acceptable image quality but also provides a large embedding capacity [11]. The results are compared with the PVD method, and the values obtained are better than the PVD method.

In 2011 In Koo Kang, Gonzalo R. Arce, Heung Kyu Lee proposed a color extended visual cryptography using error diffusion. This paper introduces a color visual cryptography encryption method that produces a meaningful color shares via visual information pixel. It is used for color images [12]. But it has poor display quality of the recovered images.

In 2012 Tasnuva Mahjabin, Syed Monowar Hossain and Md. Shariful Haque proposed data hiding method based on pixel value differencing (PVD) and least significant bit (LSB) substitution. Using PVD & LSB methods achieved an increased embedding capacity and lower image degradation also improved security [13]. An efficient and dynamic embedding algorithm was proposed here that not only hides secret data with an imperceptible visual quality and increased capacity but also make secret code breaking a good annoyance for the attacker. This feature of this method provides security of the hidden secret data.

 ISSN: 2454-4248
59 – 62

In 2013 Komal B. Bijwe proposed a shifting method with segmentation and efficient higher LSB method for data hiding with encrypted data into guard pixels region of a multicarrier image objects. We know that steganography is the science which involves secret data communicating in an appropriate multimedia carrier, e.g. data, image, audio and video files. Using this method, it is useful to hide data secretly but for the different image file formats have different methods of hiding messages [14].

In 2014 Vinit Agham proposed the novel separable scheme used for encryption. With the help of encryption it also include key [15]. Using this scheme hide large amount of data without compressing and quality of image also maintain. But according to this paper, scheme is not work if data or information is in the form of sound and video.

In 2015 Sheetal A. Kulkarni and Shubhangi B. Patil proposed a Robust Encryption Method for Speech Data Hiding in Digital Images for Optimized Security [16]. In this paper the encryption algorithm applied with embedding method is the robust secure method for data hiding**.**

III. GENREAL METHOD FOR REVERSIBLE DATA HIDING SCHEME

Steps for data flow diagram for Data hiding in an Image:

Step 1: Start
Step 2: Input cover image
Step 3: Select secret image
Step 4: Convert secret image into binary format
Step 5: Encrypt secret image by aping encryption algorithm
Step 6: Split pixels into R, G, and B channels
Step 7: Replace 5^{th} Bits with secret image binary bits for Reversible Image.
Step 8: Flip adjacent bits
Step 9: Generate new stego carrier image
Step 10: Stop.

Steps for data flow diagram for Data Extraction:

Step 1: Start
Step 2: Input encrypted stego image
Step 3: Read stego image
Step 4: Extract 5^{th} position bits
Step 5: Collect 5^{th} bit of R, G and B channels to text file
Step 6: Generates secret image
Step 7: Stop

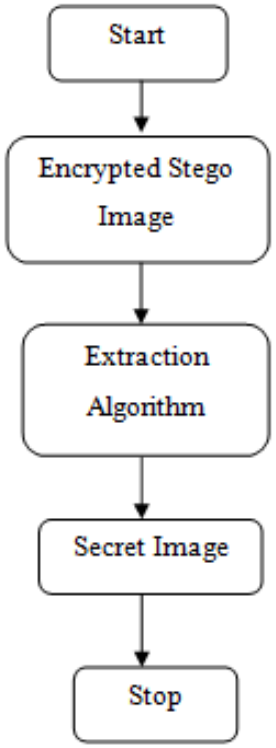

Figure 1: Flow Diagrams for Data Extraction Algorithm.

IV. CONCLUSION:

This paper gives an overview about the working of Reversible scheme for Data Hiding

REFERENCES

[1] Yeuan Kuen Lee and Ling-Hwei Chen, "An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement'', IEEE proceeding-Visual Image signal processing Volume 134, May 1999.

[2] Y. K. Lee and L. H. Chen, "High capacity image steganographic model", IEEE proceeding-Visual Image signal processing, Volume 137, June 2000.

[3] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography'', Theoretical Computational Science, volume 250, pp. 143–161, 1–2, January 2001.

[4] Chang-Chou Lin, Wen-Hsiang Tsai, "Visual cryptography for gray-level images by dithering techniques", pattern Recognition Letters 24, pp. 349–358, 2003.

[5] Tung Hsiang Liu and Long Wen Chang, "An Adaptive Data Hiding Technique for Binary Images", Proceeding IEEE 17th International Conference On Pattern Recognition (ICPR'04) 2004.

[6] H.C. Wu, N.I. Wu, C.S. Tsai and M.S. Hwang," Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEEE Proceeding Image Signal Processing, Volume 152, No. 5, October 2005.

[7] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible data hiding", IEEE Transaction Circuits System Video Technology, volume 16, no. 3, pp. 354-362, March 2006.

 ISSN: 2454-4248
59 – 62

[8] C. N. Yang and T. S. Chen, "Extended visual secret sharing schemes: Improving the shadow image quality'', International J. Pattern Recognition Artificial Intelligence, volume 21, no. 5, pp. 879–898, August 2007.

[9] Beenish Mehboob and Rashid Aziz Faruqui, "A Stegnography Implementation'', IEEE Transaction on Biometrics and security technologies, pp1-5, 2008.

[10] Amanpreet Kaur, "A New Image Steganography Based On First Component Alteration Technique", (IJCSIS) International Journal of Computer Science and Information Security, Volume 6, No. 3, pp. 53-56, 2009.

[11] M. B. Ould Medeni, "A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution'', IEEE Transaction on Multimedia computing systems pp. 1-4, 2010.

[12] In Kang, G. R. Arce, and H. K. Lee, "Color extended visual cryptography error diffusion'', IEEE Transaction Image Proceeding, volume 20, no. 1, pp. 132–145, January 2011.

[13] Tasnuva Mahjabin, "A Block Based Data Hiding Method in Images Using Pixel Value Differencing and LSB Substitution Method", IEEE 2012.

[14] Komal B. Bijwe, "An Efficient Higher LSB Method for Hiding Encrypted Data into Guard Pixels Region of a Multicarrier Image Objects", International Journal of Science and Research, Volume 2, December 2013.

[15] Vinit Agham, "Data Hiding Technique by Using RGB, LSB Mechanism", International Conference, 2014.

[16] Sheetal A. Kulkarni, "A Robust Encryption Method for Speech Data Hiding in Digital Images for Optimized Security", International Conference on Pervasive Computing, pp. 8-10 January 2015.

[17] Hao tian Wu, Jean luc Dugelay and Yun qing Shi, "Reversible Image Data Hiding with Contrast Enhancement", IEEE Signal Processing Letters, Volume 22, No. 1, January 2015.