International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Survey On: Reversible Data Hiding in Encrypted JPEG Images

N. B. Pokale[1], Sanjivani S. Koli[2]

[1]Professor, Department of Computer Engineering, Pune University, BSCOER Narhe , Pune, Maharashtra,, India

[2]Pune University, BSCOER Narhe , Pune, Department of Computer Engineering, Pune, Maharashtra, India

Abstract: ***Reversible data hiding (RDH) is just an approach where secret Data is stuck right into a cover picture in an opposite way. Generally RDH spatial-domain photographs are encrypted. The planned system encrypts the JPEG bit stream in to an adequately arranged structure. Then it embeds personal information in to the secured bit stream by gently adjusting the JPEG stream. Helpful bits ideal for knowledge hiding are then identified. It will help to effectively rule the protected bit stream holding key data. To have an ideal knowledge removal and picture recovery, error modification codes are utilized in coding the key message. Encryption and embedding keys are utilized in encryption and embedding processes. The secrete message bits are encoded with R and embedded into the encrypted bit stream by altering the appended bits. Utilizing the encryption and embedding keys, the recipient may remove the embedded information and completely recover the initial image. Once the embedding key is missing, the initial picture could be approximately recovered with adequate quality without removing the hidden data.***

Keywords: secret data, spatial-domain photographs, secured bit stream, Encryption, embedding keys**.**

1. Introduction

To hide key data in such way that data may be reversed, Reversible Knowledge Hiding (RDH) technique is used. Knowledge may be restored to its original way without the reduction and also without using any other information. This can be termed as Lossless embedding. At the receiver end, concealed data is removed and picture can also be restored in its original form. This technique is more helpful in applications by which original picture should remain unchanged despite data stuck is restored [1] [2]. For example: Multimedia store and Medical Imaging, Military for important works. In such applications, not minute change in pixel is accepted. Every little included data is important. If any change occurs then your concealed data will get affected and permission to access original data is required. Reversible data embedding can be viewed as an data carrier. It is impossible for human eyes to distinguish between stuck picture and original image. As a result of this, reversible data embedding may be thought as key communication model. Without using metadata, reversible data embedding offers true self authentication system by embedding its concept authentication rule [5]. Reversible data hiding (RDH) offers exact reconstruction of picture and also removal of data. Reversible data embedding is vulnerable against destructive strike [1] [3] [4]. Firstly reversible data embedding was presented by Honsinger1 in 1999. It was implemented for lossless authentication that was affected by obvious loss in data.

Ostensibly, by using of redundancy in the first picture Reversible Knowledge hiding (RDH) was developed. By implementing a few models of Reversible Knowledge Embedding, Kalker and Willems obtained top of the bounds of embedding capacity based on the data principle [3] [4]. A broad Reversible Knowledge Embedding model planned Fridrich that includes a space produced by compression to keep stuck key bits. In good quality data embedding strategy is to select embedding region in picture and payload and the first values are stuck in that. That quantity of data is bigger than embedding area. So it must depend on lossless data compression. Jun Tian presented Difference Growth (DE) [5], is yet another strategy by which, by discovering the redundancy in the picture it decides additional storage space. Difference Growth technique embeds a payload in to images reversibly. Difference Growth has best payload capacity restrict and the visible quality of stuck images. It has additionally a low computational complexity. Different process is Histogram Shifting (HS) [6]. In this approach, histogram of pixels is moved for hiding key bits. You will find different RDH strategies which use new prediction or problem growth algorithms [7] [8] [9] or generates RDH rule based upon theoretical expressions [10] [11].

Generally speaking RDH is employed to embed data in to images which can be open for data hider. There might n situations by which picture owner isn't prepared to talk about picture material to data hider. So it's required to add additional communications such as authentication data etc. to protected image. Buyer-Seller programs can also be implemented using Treating Knowledge Hiding technique [14]. In cases like this a supplier encrypts data and embeds an protected fingerprint written by buyer. Vendor may not able to get fingerprints of buyer and till buyer does not produce payment he'll not able to access the first edition of data. Different process by which, protected images are divided into blocks and by tossing three LSBs of half the pixels in the stop, one touch in each stop is stuck . At receiver's end, by considering the fluctuation of the pixel values in most decrypted stop, the secret portions get restored and also the first picture is recovered.

A marked improvement in this approach is completed by Hong by developing relationship of the edge between neighboring blocks, and employing a side-match system to attain a low problem charge [15]. In addition it expanded as separable RDH scheme. It is achieved by compressing the protected data employing a supply coding system with side

information. It creates data removal of data independent of security. K. Ma, W. Zhang, and X. Zhao implemented a RDH technique by which some rooms before security is reserved [16]. For that, employing a old-fashioned RDH process, LSBs of some pixels are first stuck in to different pixels. Then picture is encrypted. For embedding data with the information portions, positions of these LSBs in the protected picture are used.

2. Literature Review

In this paper [12], a weight based prediction scheme is presented to improve the performance of many reversible histogram-based data hiding approaches. By research the answer of the least-squares problem, we obtain the optimal set of loads for the neighboring pixels to enhance the prediction accuracy of the the prospective pixel across the entire image. The levels of the peak points in the histogram can then be elevated to boost the embedding capacity. Experiments of our implemented algorithm had been done over many well-known test images. They had proved that their planned technology significantly improves the embedding volume upon many techniques and still retains the caliber of Stego-images.

A novel reversible data hiding approach in protected photographs is shown in this paper [13]. Rather than embedding data in protected photographs immediately, some pixels are projected before security to ensure that additional data may be embedded in the calculating errors. A standard security algorithm like Advance encryption slandered is placed on the remaining pixels of the picture and a particular security scheme is made to encrypt the calculating errors. Without the security key, one can't get access to the initial image. Nevertheless, given the data hiding key only, he is able to introduce in or extract from the protected picture additional data without knowledge about the initial image. Moreover, the knowledge removal and picture recovery are free of errors for many images. Studies display the feasibility and performance of the planned strategy, particularly in part of embedding charge versus Peak Signal-to-Noise Ratio (PSNR).

A novel reversible knowledge hiding algorithm, which can recover the initial image without the distortion from the noted image following the hidden knowledge have already been extracted, is shown in this paper. This algorithm [6] utilizes the zero or the minimum details of the histogram of a picture and slightly modifies the pixel grayscale prices to introduce knowledge into the image. It can introduce more knowledge than lots of the current reversible knowledge covering algorithms. It is shown analytically and found experimentally that the peak signal-to-noise percentage (PSNR) of the noted image produced by this method versus the initial image is fully guaranteed to be above 48 dB. 0

That decrease bound of PSNR is much greater than that of most reversible knowledge covering practices noted in the literature. The computational complexity of our proposed technique is minimal and the execution time is short. The algorithm has been effectively placed on a wide variety of photos, including typically applied photos, medical photos, structure photos, aerial photos and each of the 1096 photos in CorelDraw database. Experimental effects and efficiency contrast with different reversible knowledge covering schemes are shown to demonstrate the validity of the algorithm.

In that report [10], the optimal principle of value adjustment below a payload-distortion principle is found by using an iterative technique, and a functional reversible information hiding scheme is proposed. The key information, along with the additional information used for content recovery, are carried by the differences between the first pixel-values and the equivalent values estimated from the neighbors.

Here, the estimation problems are modified based on the optimal price transfer rule. Also, the host picture is divided into a number of pixel subsets and the reliable information of a subset is always embedded in to the estimation problems within the next subset. A receiver can properly remove the embedded secret information and recover the first content in the subsets by having an inverse order. This way, a great reversible information hiding efficiency is achieved.

3. Conclusion

In this paper, we have stated Reversible Information Hiding that will be used to hide information in photos or protect media and secured JPEG bitstream. For covering the image content, the first JPEG bitstream is correctly encrypted. The bitstream structure is also maintained in that technique. With ECC, The secret message bits are encrypted. Then by adjusting the appended bits corresponding to the AC coefficients, key messages are embedded into the secured bitstream. The device may remove embedded knowledge applying security and embedding keys. The initial tips may be restored accurately. Image may be restored also though the embedding essential is absent.

This paper addresses existing techniques for that and also addresses new improvements in recent technique. In this paper, we have matters like Bitstream Encryption, JPEG Bitstream Parsing, and Component of Information covering process, reversible knowledge covering.

References

[1] J. Fridrich and M. Goljan, “Lossless data embedding for all image formats,” in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.
[2] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, “Reversible watermarking algorithm using sorting and prediction,” IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.
[3] T. Kalker and F.M.Willems, “Capacity bounds and code constructions for reversible data-hiding,” in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.
[4] F. M.Willems and T. Kalker, “Coding theorems for reversible embedding,” DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 66, pp. 61–78, 2004.

[5] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896 Aug. 2003.
[6] Z. Ni, Y. Shi, and N. Ansari et al., "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.
[7] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.
[8] L. Luo et al., "Reversible image watermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.
[9] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.
[10] X. Zhang, "Reversible data hiding with optimal value transfer," IEEE Trans. Multimedia, vol. 15, no. 2, pp. 316–325, 2013.
[11] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.
[12] Shih-Lun Lin, "Improving Histogram-based Reversible Information Hiding by an Optimal Weight-based Prediction Scheme", Journal of Information Hiding and Multimedia Signal Processing, Ubiquitous International, Volume 4, Number 1, January 2013
[13] Weiming Zhang, Kede Ma, Nenghai Yu," Reversibility improved data hiding in encrypted images ", Published by Elsevier B.V, Signal processing 94 (2014) 118-127
[14] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.
[15] 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.
[16] K. Ma, W. Zhang, and X. Zhao et al., "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, 2013.