Survey of Reversible Data Hiding using Chaos and Genetic Algorithm in Encrypted JPEG Bitstream

Vaibhav Sonyabapu Barve[1], S. S. Bere[2]

[1]ME Student, Department of Information Technology,
Dattakala Group of Institute of Technology, University of Pune, Pune, Maharashtra, India

[2]Assistant Professor, Department of Information Technology,
Dattakala Group of Institute of Technology, University of Pune, Pune, Maharashtra, India

Abstract: ***Reversible data hiding (RDH) is a technique where secret Information is embedded into a cover image in a reverse way. In general RDH spatial-domain images are encrypted. The proposed system encrypts the JPEG bit stream into a properly organized structure. Then it embeds private message into the encrypted bit stream by lightly changing the JPEG stream. Useful bits suitable for data hiding are then identified. This helps to accurately code the encrypted bit stream carrying secret data. To have a perfect data extraction and image recovery, error correction codes are used in encoding the secret message. Encryption and embedding keys are used in encryption and embedding processes. The secret message bits are encoded with RC4 and embedded into the encrypted bit stream by modifying the appended bits. By using the encryption and embedding keys, the receiver can extract the embedded data and perfectly restore the original image. When the embedding key is absent, the original image can be approximately recovered with satisfactory quality without extracting the hidden data.***

Keywords: Reversible data hiding, JPEG bit stream, RC4, Embedding.

1. Introduction

To hide secret data in such manner that data can be reversed, Reversible Data Hiding (RDH) technique is used. Data can be restored to its original manner without any loss and also without using any other information. This can be termed as Lossless embedding. At the receiver end, hidden data is extracted and image is also restored in its original form. This technique is more useful in applications in which original image should remain intact even after data embedded is retrieved [1] [2]. For example: Military and Medical Imaging, Multimedia archive for valuable works. In such applications, not minute change in pixel is accepted. Every bit of embedded data is important. If any change occurs then the hidden data will get affected and raw data, access to original is required. Reversible data embedding can be viewed as an information carrier. It is impossible for human eyes to distinguish between embedded image and original image. Because of this, reversible data embedding can be thought as secret communication model. Without using metadata, reversible data embedding gives true self authentication scheme by embedding its message authentication code [5]. Reversible data embedding (RDH) provides accurate reconstruction of image and also extraction of data. Reversible data embedding is susceptible against malicious attack [1] [3] [4]. Firstly reversible data embedding was introduced by Honsinger1 in 1999. It was implemented for lossless authentication which was affected by visible loss of data.

Basically, by using of redundancy in the original image Reversible Data Embedding (RDH) was developed. By implementing several models of Reversible Data Embedding, Kalker and Willems obtained the upper bounds of embedding capacity based on the information theory [3] [4]. A general Reversible Data Embedding model proposed Fridrich which has a room created by compression to hold embedded secret bits. In high quality data embedding approach is to select embedding area in image and payload and the original values are embedded in that. This amount of information is larger than embedding area. So it has to depend on lossless data compression. Jun Tian introduced Difference Expansion (DE) [5], is another approach in which, by exploring the redundancy in the image it determines extra storage space. Difference Expansion technique embeds a payload into images reversibly. Difference Expansion has best payload capacity limit and the visual quality of embedded images. It has also a low computational complexity. Other method is Histogram Shifting (HS) [6]. In this method, histogram of pixels is shifted for hiding secret bits. There are other RDH methods which use new prediction or error expansion algorithms [7] [8] [9] or generates RDH code depending upon theoretical expressions [10] [11].

In general RDH is used to embed data into images which is open for data hider. There may b situations in which image owner is not ready to share image content to data hider. So it is necessary to append extra messages such as authentication information etc. to encrypted image. Buyer-Seller systems are also can be implemented using Reversing Data Hiding technique [12] [13] [14]. In this case a seller encrypts data and embeds an encrypted fingerprint given by buyer. Seller will not able to get fingerprints of buyer and until buyer does not make payment he will not able to access the original version of data. Other method in which, encrypted images are divided into blocks and by flipping three LSBs of half the pixels in the block, one bit in each block is embedded [15]. At receiver’s end, by analyzing the fluctuation of the pixel values in every decrypted block, the secret bits get retrieved and also the original image is recovered. An improvement in this method is done by Hong by developing correlation of the border between neighboring blocks, and using a side-match scheme to achieve a low error rate [16]. It also extended as separable RDH scheme. It is accomplished by compressing the encrypted data using a source coding scheme with side information. It makes data extraction of data independent of encryption [17]. K. Ma, W. Zhang, and X. Zhao implemented a RDH technique in which some rooms before encryption is reserved [18]. For that, using a traditional RDH method, LSBs of some pixels are first embedded into other pixels. Then image is encrypted. For embedding information with the data bits, positions of these LSBs in the encrypted image are used.

2. Literature Review

Literature review is classified into Reversible data hiding, Component of Data hiding process, JPEG Bitstream Parsing, Bitstream Encryption.

1) Reversible Data Hiding

The process of hiding of data into images or media which also represents information is called as Data Hiding. The data hiding is connected with two data sets. Those are a set of embedded data and set of cover media data. Depending upon relationship between these two sets of data, applications are distinguished. For example: in secret communications, the hidden data is often not related to cover media. In applications such as authentication, data and cover media are often related. In both of these applications, hiding of data is necessary factor. In data hiding, it is seen that distortion is present the image or cover media. This happens because of hiding of data and it is not restored back to its original form. Permanent distortion can happen to data of cover media even though hidden data have been extracted out. In applications used in law enforcement and medical diagnosis, after retrieving hidden data for some legal considerations it is important to get cover media back in its original form. Techniques which can reverse back the cover media into its original form are known as lossless, invertible, reversible or distortion free data hiding techniques. Reversible data hiding techniques enables huge chance to link two sets of data. Due to this cover media can be losslessly recovered after extraction of hidden data. Also provides extra way to handle both sets of data [6].

2) Component of Data hiding process

There are mainly three components present in entire workflow of encryption-embedding-extraction-restoration.

3) Content owner

Content owner selects or chooses an encryption key. Content owner converts original JPEG bitstream. Also encrypts bitstream for hiding data of original image. To be decoded appropriately to its undistorted image, it is necessary for encrypted bitstream to have same structure as the original.

4) Data hider

A secret message is embedded into the encrypted JPEG bitstream by data hider. It chooses appropriate places to hide data into image. Depending on it, achievable embedding capacity calculated. Using error correction codes (ECC), plain bits are encrypted into secret bits. The word *plain* is linked with original message to be transmitted. Same as of word *secret* is linked with ECC-encoded and encrypted secret bits. Data-hider uses an embedding key for security.

5) Receiver

A secret message is extracted by Receiver. It also gets back the JPEG bitstream. Secret bits are extracted and decrypted into plain bits by using both embedding and encryption key. Also original JPEG bitstream is accurately restored. An image can be retrieved even though the receiver only has the encryption key.

6) JPEG Bitstream Parsing

An image can be divided as set of quantized DCT coefficients in non-overlapped blocks. After that coded into bitstream with entropy encoding, as per JPEG standard [19]. DC and AC coefficients are handled independently, during entropy encoding. After using one dimensional predictor, coefficients are encoded by using Huffman codes. In case of AC coefficients, the coefficients are proficiently encoded with the run length coding (RLC) as there are number of zero's. In the JPEG file header, tables of Huffman/VLC coding and quantization are defined and stored. For entropy encoding and decoding, these tables are important. By using Huffman codes and the corresponding appended bits, the entropy encoded bits are structured. Bitstream parsing examines compressed bits with respect to the JPEG structure and the Huffman tables retrieved from the JPEG file header.

7) Bitstream Encryption

Our aim is by using a JPEG decoder; encrypt a JPEG bitstream into a form which can be decrypted directly into unidentifiable image. A modification on single bit may cause failure of decrypting, because JPEG data has strict structure. To develop a JPEG encryption scheme, special caution has to be taken in present work. For that, by selecting and modifying the changeable bits, encryption should be obtained. The encryption process contains of two stages:

1. Encryption of the appended bits
2. Encryption of the quantization table.

3. Conclusion

In this report, we have surveyed a Reversible Data Hiding which is used to hide secret in images or cover media and encrypted JPEG bitstream. For hiding the image content, the original JPEG bitstream is correctly encrypted. The bitstream structure is also preserved in this technique. With ECC, The secret message bits are encrypted. Then by changing the appended bits matching to the AC coefficients, secret messages are embedded into the encrypted bitstream. The receiver can extract embedded data using encryption and embedding keys. The original keys can be restored accurately. Image can be restored even though the embedding key is absent. This report covers existing techniques for that and also covers new improvements in current technique. In this paper, we have surveyed topics like Reversible data hiding, Component of Data hiding process, JPEG Bitstream Parsing, Bitstream Encryption.

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 imagewatermarking 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] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. Image Process.*, vol. 10, no. 4, pp. 643–649, Apr. 2001.

[13] M. Deng, T. Bianchi,A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in *Proc. 11th ACM Workshop Multimedia and Security*, 2009, pp. 9–18.

[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] X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[16] 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.

[17] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[18] 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.