Reversible Data Hiding in Encrypted JPEG Bitstream

Priyanka Dighe
Pravara Rural Engineering College,Loni,Maharashtra, India.

Khade Nalini
Pravara Rural Engineering College,Loni,Maharashtra, India.

G.R.Suryawanshi
Pravara Rural Engineering College,Loni,Maharashtra, India.

Abstract— This consistency proposes a framework ofvarying data obnubilating (RDH) in an encrypted JPEG bitstream.Unlike subsisting RDH methods for encrypted spatial-domainimages, the proposed method aims at encrypting a JPEGbitstream into an opportunely organized structure, and embedding asecret message into the encrypted bitstream by scarcely modifyingthe JPEG stream. We identify utilizable bits congruous for data obnubilatingso that the encrypted bitstream carrying private datacan becorrectly decoded. The private message bits are encoded witherror rectification codes to achieve an impeccable data extraction andimage recuperation. The encryption and embedding are controlled byencryption and insert keys properly. If a receiver hasboth keys, the secret bits can be extracted by analyzing theblocking artifacts of the neighboring blocks, and the pristinebitstream impeccably recuperated. In case the receiver only has theencryption key, he/she can still decode the bitstream to obtain theimage with good quality without extracting the obnubilated data.

Keywords— Encrypted image, image recovery, information hiding, JPEG, reversible data hiding . Graphical password, cloud security .

1. INTRODUCTION

Reversible data obnubilating (RDH) is a technique that embeds secret information into a cover image in a reversible manner. On the receiving side, the obnubilated message can be extractedand the pristine image impeccably renovated. This technique is especially subsidiary in applications such as medical and military imaging where the pristine image must not be modified after the embedded data are extracted [1], [2]. Unlike robust watermarking, RDH accentuates perfect image reconstruction and data extraction, but not the heftiness against maleficent attacks [1], [3], [4]. This is subsidiary, for example, in cloud storage. When a database manager endeavors to label the files utilizing RDH methods, no transmission is involved, consequently no errors and attacks either. Essentially, RDH is realized by making use of redundancy in the pristine image. Kalker and Willems established several models for RDH, and derived the upper bounds of embedding capacity for different applications predicated on the information theory [3], [4]. One popular approach is the difference expansion (DE) method in which inequality of pixel groups are calculated and expanded to accommodate supplemental bits [5]. Another is the histogram shifting (HS) that obnubilates secret bits by shifting the histogram of pixelvalues [6]. Other RDH methods have been proposed to ameliorate embedding efficiency, e.g., the schemes making utilization of incipient prognostication or error expansion algorithms [7]–[9], or engendering RDH codes according to the theoretical expressions of RDH[1], [2]. Generally, these RDH methods are utilizable for embedding data into images that are open to the data-hider. In some applications, however, the image owner may be reluctant to disclose the image contents to the data-hider. For example, the patient's secret information must not be revealed to the person who embeds data into the medical image, while the pristine image must be impeccably recuperated and the embedded data thoroughly extracted on the receiver end. In this case, the channel provider has to append adscititious messages such as image metadata, notation and authentication information to the encrypted version of the pristine images.

RDH in encrypted images is withal congruous for the buyer-seller system [3]–[4]. The seller of digital multimedia content encrypts the pristine data and embeds an encrypted dactylogram supplied by the client. In this case, the seller cannot obtain the client's dactylogram, and the buyer cannot access the pristine version unless he/she makes the payment to consummate the transaction.

Some methods of RDH in encrypted pictures have been intended. In [2], Zhang divides the encrypted image into blocks, and embeds one bit into each slab by flipping three LSBs of half the pixels in the block. On the receiver side, the secret bits are extracted and the pristine pictures recuperated by analyzing the fluctuation of the pixel values in all decrypted block. Zhang further proposed a separable RDH scheme for encrypted images by compressing the encrypted data utilizing a source coding scheme with side information, making data extraction independent of encryption [17]. Recently, Ma et al. proposed an RDH method for encrypted pictures by reserving some room afore encryption [1]. To do so, LSBs of some pixels are first embedded into other pixels

utilizing a traditional RDH method, and the image is then encrypted. As a result, positions of these LSBs in the encrypted picture can be used for embedding information with the data-hider. As JPEG is widely utilized, in this correspondence we propose a novel RDH framework to obnubilate data in an encrypted JPEG bitstream. The scheme is defined to fluster the principal content of the pristine image while preserving the bitstream structure. The secret bits are encodedwith error rectification codes and then embedded into the JPEG bitstream. On the receiving side, slabing artifacts of neighboring blocks are used to extract the secret bits and impeccably instaurate the pristine bitstream.

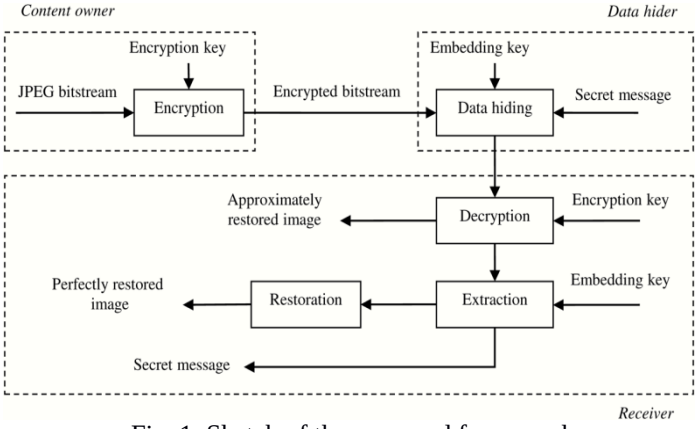

Fig. 1. Sketch of the proposed framework.

2. RELATED WORK

The general framework of the proposed scheme is adumbrated in Fig. 1. Consider the three parties in the entire workflow of encryption-embedding- extraction-renovation: content owner, data hider, and receiver, whose roles are described as follows. Content owner: Parse the pristine JPEG bitstream and encrypt the bitstream to conceal the principal content of the pristine image. An encryption key is culled by the content owner. The encrypted bitstream must have the same structure as the pristine so that it can be decoded correctly to give an undistorted image. Data hider: Embed the secret message into the encrypted JPEG bitstream. Congruous positions for data obnubilating are culled, and the achievable embedding latitude calculated. Encode plain bits into secretbits with error rectification codes (ECC). The word plain is associated with the pristine message to be transmitted, and secret corresponds to the ECC-encoded and encrypted secret bits. An embedding key is utilized by the data- hider for security. Receiver: Extract the secret message and instaurate the JPEG bitstream. With both the encryption key and embedding key, the secret bits are extracted and decoded into plain bits, and the pristine JPEG bitstream is impeccably renovated. If the receiver only has the encryption key, an image with good quality can still be obtained approximately.

3. PORPOSED MODELLING

BITSTREAM PARSING AND ENCRYPTION

JPEG Bitstream Parsing According to JPEG standard [5], an image is decomposed to a set of quantized DCT coefficients in non-overlapped blocks, and then coded into a bitstream with entropy encoding. During entropy encoding, the DC coefficients and the AC coefficients are handled discretely. The DC coefficients are coded with the Huffman codes after utilizing a unidimensional presager. For AC coefficients, since there are many zeros, the coefficients are efficiently encoded with the run length coding (RLC). The quantization tables and Huffman/VLC coding tables are defined and stored in the JPEG file header, which are vital for entropy encoding and decoding. The entropy encoded bits are structured by the Huffman codes and the analogous appended bits, as shown in Fig. 2, in which the Huffman code identifies the range of the coefficient magnitude and the length of appended bits. Bitstream parsing is a component of the entropy decoding, which investigate the compressed bits according to the JPEG structure and the Huffman tables extracted from the JPEG file header.

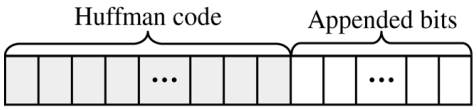

Fig. 2. Encoding structure for each coefficient.

Bitstream Encryption

We aim at encrypting a JPEG bitstream into the one that can be decoded into an unrecognizable image directly by a JPEG decoder.Due to the stringent structure of JPEG data, any alteration on individual bit may cause the failure of decoding. Consequently, special care is takenin the present task to devise a JPEG encryption scheme. For that purport, we do the encryption according to the encoding structure by culling and modifying the mutable bits. The encryption procedure consists of two steps, encryption of the modified bits and encryption of the quantization table.

Fig. 3. JPEG bitstream encryption: the left is original, and the right encrypted.

The template is utilized to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not modify them. You may note peculiarities. For example, the head margin in this template measures proportionately extra than is customary. This quantification and others are deliberate, utilizing designations that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

4. RESULTS AND DISCUSSIONS

All images used in the experiments are standard gray-scale images sized 512 × 512. We compress these into JPEG bitstreams utilizing different quality factors. LDPC codes are utilized for error rectification utilizing the parity-check matrix proposed in [20] to engender LDPC codes, in which n k = 396 / 150, and the credence propagation algorithm is utilized in LDPC decoding. Details of the LDPC algorithm can be found in [21]. Fig. 6 gives an example where (a) is the pristine JPEG image with a quality factor Q = 80, and (b) is an encrypted image carrying secret data, which contains 1980 secret bits (C e = 1980) obtained from 750 message bits utilizing LDPC codes. The image in (c) is decrypted from the received bitstream utilizing the encryption keys K enc - 1 and K enc - 2 . The results are horrible when we commence testing. The environment needed an abundance of tuning like Software and hardware compatible issues. After we had _nished tuning the environment, we were able to commence getting all the tests to prosper (no errors re- ported by the testing implement). Then we commenced to get results. These results have been recorded in the referenced PDF. During the _nal phase or testing, we consummated total or 4 tests. Each subsequent test incremented both the number of concurrent users and the overall length or the test.

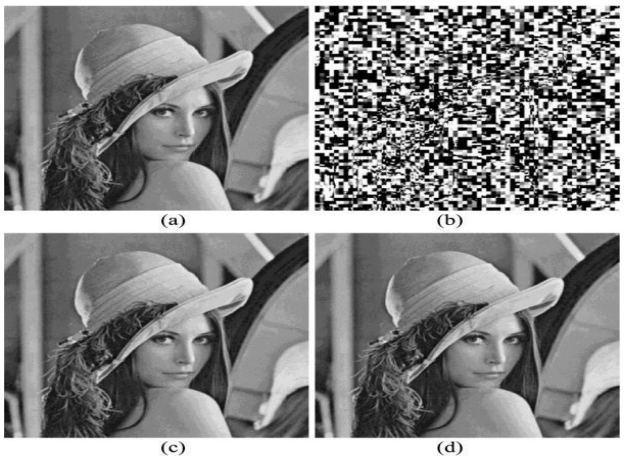

Fig. 6. Encryption and image recovery: (a) orginal JPEG image,(b) encrypted image carrying secret data, (c) decrypted, and (d) recovered.

TABLE I

EMBEDDING CAPACITY (BITS) OF JPEG BITSTREAM FOR ERROR-FREE XTRACTION WHEN QUALITY FACTOR EQUALS 80, 50, AND 20, RESPECTIVELY.

Image	Q=80		Q=50		Q=20	
	C_e	C_p	C_e	C_p	C_e	C_p
Lena	1980	750	1584	600	1188	450
Baboon	1980	750	1980	750	1980	750
Pepper	1980	750	1584	600	1188	450
Sailboat	1980	750	1584	600	1584	600
Man	1980	750	1584	600	1584	600
Couple	1980	750	1980	750	1584	600
Barbara	1980	750	1584	600	1188	450
Goldhill	1980	750	1980	750	1584	600

PSNR of (c) is 38.0 dB with deference to (a). After extracting the embedded 750 message bits from (c), the pristine image is impeccably recuperated as shown in (d), which is identical to (a). Table I lists embedding capacities (in bits) of the tested JPEG images, utilizing quality factors 80, 50, and 20, respectively. The embedding capacity and the net capacity are calculated according to n / k of the LDPC codes, which is culled for each image to ensure that no error occurs in the extracted message. The number of utilizable blocks changes corresponding to different quality factors. The more immensely colossal the quality factor, the more blocks are utilizable for data obnubilating. Net capacity of JPEG bitstream is always constrained by image compression and encryption. Nonetheless, this caliber of payload is ample formany practical utilization, e.g., defining a 512 × 512 sized image utilizing dozens of characters, or obnubilating several hundred authentication bits for image bulwark. When utilizing blocking artifacts for data extraction, error may transpire in the judgment. Fig. 7 shows precision of extracting bits from the bitstream carrying secret data, corresponding to different quality factors.

TABLE II

EMBEDDING CAPACITY (BITS) OF IMAGES WITH DIFFERENT RDH METHODS

Images	Proposed Method	Method in [15]	Method in [16]	Method in [22]
Lena	750	1024	1024	[100, 131072]
Baboon	750	256	334	[100, 131072]
Man	750	655	1024	[100, 131072]
Sailboat	750	655	1024	[100, 131072]

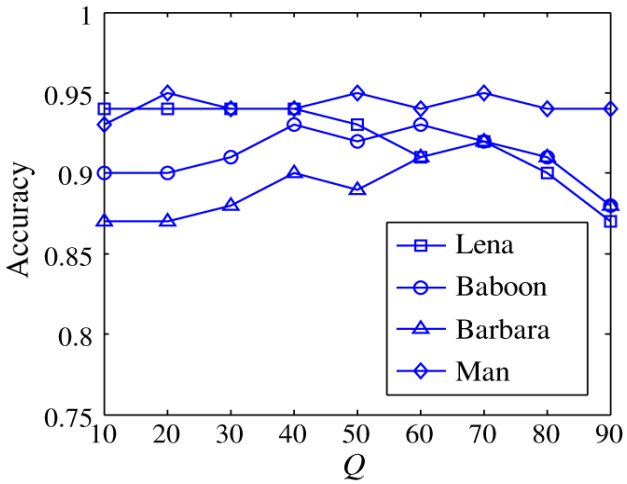

Fig. 7. Accuracy of extracted hidden data using blocking artifacts before error correction, corresponding to different quality factors.

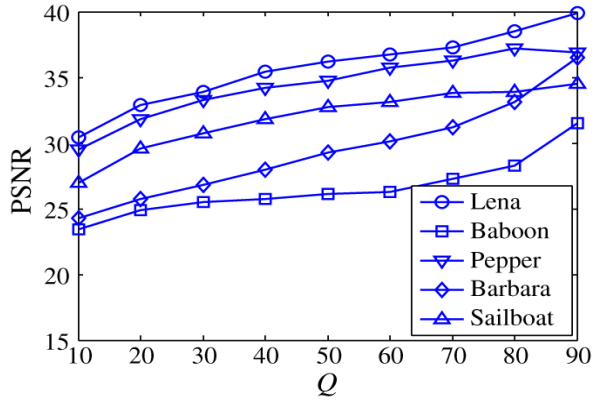

Fig. 8. Quality of decrypted images at different JPEG quality factors.

In most cases, extraction precision is proximate to 0.9, betokening minute error probability of data extraction. These errors can be eliminated by LDPC decoding, thus exhibiting efficacy of utilizing blocking artifacts in the data extraction. If the receiver does not have the embedding key, but possessethe encryption keys only, the image can still be decrypted from the encrypted bitstream, naturally with some distortion. Fig. 8 shows PSNR of the decrypted image corresponding to different JPEG quality factors. It is observed that, compared to the pristine JPEG image, quality of the decrypted image is good, and the higher the factor, the better the quality of decrypted image. Because the reversible data obnubilating methods for encrypted JPEG bitstream are very infrequent, we compare the proposed method with some reversible data obnubilating methods for plaintext-JPEG or encrypted-uncompressed images. We utilize the quality factor 80 for image compression. Experimental results of the approaches are listed Table II. Capacity of the proposed method is proximate to those in the methods [5] that we developed for reversibly obnubilating data into the encrypted data of uncompressed images. Method [3] has the variable capacity for JPEG images, which is better than the proposed method. However, the JPEG images utilized in [3] are in plaintext form, and the file sizes are consequential enlarged when the payloads are high.

5. CONCLUSION

There are several algorithms for steganography like LSB (least signi_cant bit algorithm), RLSB (Desultory least signi_cant bit algorithm). In which assailant can facilely detect the presence of obnubilated image. To surmount these quandaries incipient algorithm ELSB (Edged Predicated Least Signi_cant Bit) is proposed. This algorithm obnubilates the data inside the edge pixels. The proposed algorithm is applicable to all types of image and can be utilized in covert communication, obnubilating secret information like copyrights, trade secrets and much more. To make this more involute here we have proposed 3 tier graphical password authentication system along with it to access that image. This technique has been proven better than the alphanumeric password since last few years. In this correspondence, we propose an RDH framework for encrypted JPEG bitstream. The pristine JPEG bitstream is opportunely encrypted to obnubilate the image content with the bitstream structure preserved. The secret message bits are encoded with ECC and embedded into the encrypted bitstream by modifying the modified bits corresponding to the AC coefficients. By utilizing the encryption and embedding keys, the client can extract the embedded data and impeccably recuperate the pristine image. When the embedding key is absent, the pristine image can be approximately recuperated with copacetic quality without extracting the obnubilated data.

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] Authentication Using Graphical Passwords: E_ects of Tolerance and Image Choice (Susan Wiedenbeck, Jean-Camille Birget, Alex Brodskiy).

[4] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[5] 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.

[6] A Survey on Recognition-Based Graphical User Authentication Algorithms FarnazTowhidi Centre for Advanced Software Engineering, University Technology Malaysia Kuala Lumpur, Malaysia.