International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

Reversible Watermarking Based On Encryption Image Classification and Dynamic Color Techniques

Zara Firdouse & Ch Vani
Pg Scholar [1] Assistant Professor[2]
Department Of Ece,Nova College Of Engineering And Technology

ABSTRACT—*There are also a number of works on data hiding in the encrypted domain. The reversible data hiding in encrypted image is investigated in. Most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain.This 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. Thus the data hider can benefit from the extra space Emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images. Experiments show that this method can retrieve the same image quality .The data extraction and image recovery can be achieved by examining the block smoothness. After encrypting the entire data of an uncompressed image by a stream cipher, Image can be encrypted by different color shares According to the selected colors, with the aid of spatial correlation in natural image, the embedded data can be successfully extracted and the original image can be perfectly recovered.*

Index Terms— Reversible data hiding, image encryption, privacy protection, color histogram , watermarking, Content authentication

I. INTRODUCTION. DATA HIDING [1] is referred to as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. The relationship between these two sets of data characterizes different applications. For instance, in covert communications, the hidden data may often be irrelevant to the cover media. In authentication,

however, the embedded data are closely related to the cover media. In these two types of applications, invisibility of hidden data is an important requirement. In most cases of data hiding, the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. That is, some permanent distortion has occurred to the cover media even after the hidden data have been extracted out. In some applications, such as medical diagnosis and law enforcement, it is critical to reverse the marked media back to the original cover media after the hidden data are retrieved. Some legal considerations. In other applications, such as remote sensing and high-energy particle physical experimental investigation, it is also desired that the original cover media can be recovered because of the required highprecision nature. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free, or invertible data hiding techniques. Reversible data hiding facilitates immense possibility of applications to link two sets of data in such a way that the cover media can be losslessly recovered after the hidden data have been extracted out, thus providing an additional avenue of handling two different sets of data. With regard to providing confidentiality for images, encryption [12] is an effective and popular means as it converts the original and meaningful content to incomprehensible one. Although few RDH techniques in encrypted images have been published yet, there are some promising applications if RDH can be applied to encrypted images. In [13], Hwang et al. advocated a reputation-based trust-management scheme enhanced with data coloring (a way of embedding data into covers) and software watermarking, in which data encryption and coloring offer possibilities for upholding the content owner's privacy and data integrity. Obviously, the cloud service provider has no right to introduce permanent distortion during data coloring into encrypted data. Thus,a reversible data coloring technique based on encrypted data is preferred. Suppose a medical image database is stored in a data center, and a server in the data center can embed notations into an encrypted version of a medical image through a RDH technique. With the notations, the server can manage the image or verify its integrity without having the knowledge of the original content, and thus the patient's privacy is protected. On the other hand, a doctor, having the cryptographic key, can decrypt and restore the image in a reversible manner for the purpose of further diagnosing .Some attempts on RDH in encrypted images have beenmade.In [16], Zhang divided the encrypted image into several

blocks.By flipping 3 LSBs of the half of pixels in each block, room can be vacated for the embedded bit. The data extraction and image recovery proceed by finding which part has been flipped in one block. This process can be realizedwith the help of spatial correlation in decrypted image. Hong et al. [17] ameliorated Zhang's method at the decoder side by further exploiting the spatial correlation using a different estimation equation and side match technique to achieve much lower error rate. These two methods mentioned above rely on spatial correlation of original image to extract data. That is, the encrypted image should be decrypted first before data extraction. The proposed method separate data extraction from image decryption but also achieves excellent performance in two different prospects: • Real reversibility is realized, that is, data extraction and image recovery are free of any error. • For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved.

II. PREVIOUS ARTS A large amount of information is being transmitted over the internet, not only text but image, audio, video and other multimedia files also. Images are widely used in daily life, so security of Image data is an important requirement. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. Text steganography is considered to be the most difficult kind of steganography due to the lack of redundancy in text as compared to image or audio. However, it requires less memory and provides for simpler communication. Steganography provides a means of secret communication which cannot be removed without significantly altering the data in which it is embedded. The embedded data will be confidential unless an attacker can find a way to detect it. So attacker easy to find data's.Because that modules RSA algorithm used. In the existing system are used to cryptography concept for hides the content of the messages only don't hide the existence of the messages. • To hide the data in particular bit using public key, so easily extract the original messages. The receiver decrypts the original image and embedded data using the single key only. • In the existing System more attention is paid to reversible data hiding (RDH) in encrypted images,since it maintains the excellent property that the original cover can be lossless

Recovered after embedded data is extracted while protecting the image content's confidentiality. • All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image. • Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. The main disadvantages are: The hackers recover the embedding data in original image because the data placed in particular bit position.To attack the hidden data using original image[3] because referred the key value. The data extraction is not separable from the content descriptions. The hackers recover the embedding data in original image because the data placed in particular bit position.Previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. To attack the hidden data using original image because referred the key value.

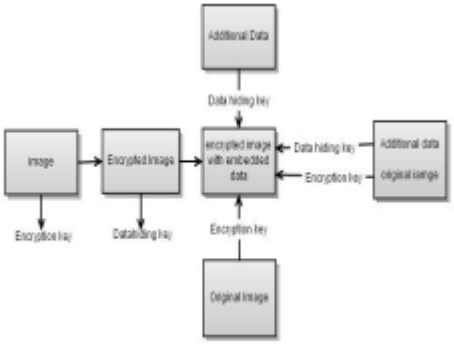
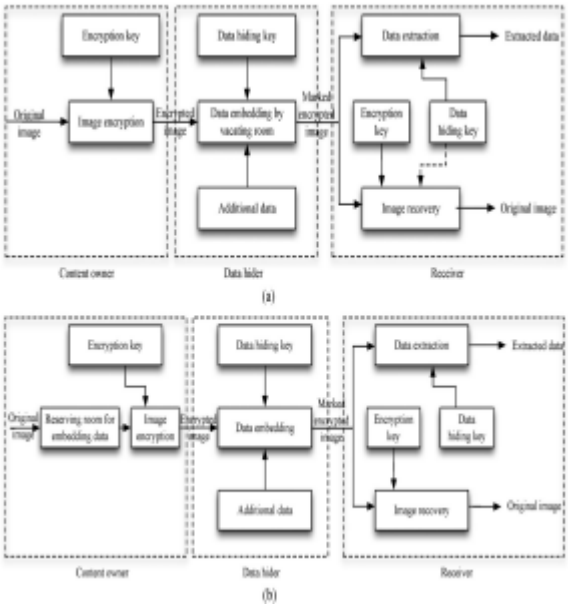


Fig 2.1 Existing system architecture

III .PROPOSED METHOD This method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. This method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.[12]This 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.We can achieve real reversibility, that is, data extraction and image recovery are free of any error. In the proposed system used steganography concept for hide the content of messages and existence of the message. The original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using a data-hiding key. In

this paper, proposes a novel scheme for separable reversible data hiding in encrypted image[7].Then, a data-hider may compress the least significant bits of the encrypted image using a datahiding key to create a sparse space to accommodate some additional data. This method can achieve real reversibility, that is, data extraction and image recovery are free of any error.It is easy for the data hider to reversibly embed data inthe encrypted image.This method can embed more than 10 times as large payloads for the same image quality and high security as the previous methods[9]. Fig.3.1 Framework: "vacating room after encryption (VRAE)" versus framework: "reserving room before encryption (RRBE)." (Dashed line in (a) states that the need of data hiding key in image recovery varies in different practical methods). (a) Framework VRAE. (b) Framework RRBE. A.Generation of encryption images This module describes the encryption of image to be transmitted. Here we use visual cryptography algorithm for encrypt the image. So first the image is converting into streams of data array and each data will be encrypted. The shares will be created based on the number of users. For example if 5 users are there means we create five shares. For each share the user can reveal the image but only after five shares he can view the full image. This algorithm not uses the encryption key because if the key is obtained by some unauthorized person then he will reveal the image very easily. B.Data Embedding This module describes about the embedding the data for secret sharing. It takes one random encrypted image.[11] Watermark gives the identification of the provider. Here we use LSB algorithm for data embedding. Before data hiding we first encrypt the data using secret key.The embedding technique of watermark is given as follows Assume that the size of the host image is 512×512. Host image is divided into small M×M blocks Z, block Z is divided into small M ×M blocks Y. If M=8 is used, the size of block Y is 8×8.



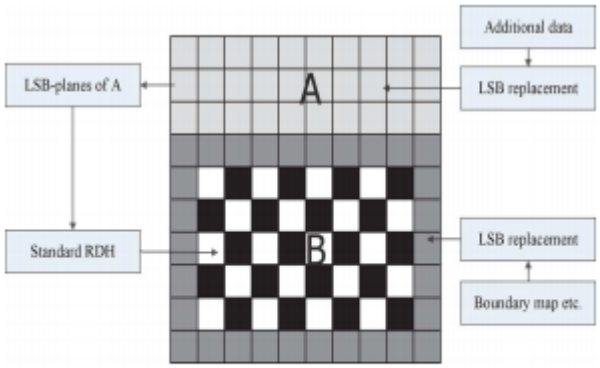


Fig. 3.2. Illustration of image partition and embedding

A number of pairs of coefficients (A,B) in block Y are chosen as A = a1, . . . , an,B = b1. . . bn based on pseudo-random numbers, and mapping key that containsindex of original chosen coefficients are kept. For embedding, two coefficient values (ai, bi) are modified by add parameter which is a parameter for watermark strength. i=1,…,n. Continue the above process according to n. Each block Y is embedded 1 bit watermark and watermark length decides how many blocks Y is embedded.

C.Data Protection Image retrieval is computationally intensive and can benefit from offloading to save energy. To handle the protected data, the image retrieval program may be modified; the modified program must provide acceptable retrieval performance compared with the original program. And unprotected data. Different retrieval algorithms may need different protection schemes. We consider two retrieval algorithms:[8] ImgSeek and Gabor filtering, and two protection schemes: Steganography and homomorphism encryption. Steganography uses a cover image todisguise the secret image so that it is difficult to detect.A simple and commonly used image Steganography technique is hiding images by replacing bits from the coverimage with bits from the secret image. Encryption transforms plain data to make them unreadable. Steganography is different from encryption: the former hides the existence of data. In contrast, encryption makes the data meaningless without the key.

D. Data Encryption Encrypt Image: the input image is encrypted using a encryption key before the compression of image. by which can a image is restricted to view from the unauthorized user access. Embed Data: In the image the data is embedded after compressing the image by using appropriate technique. The message is embed in to the image using a data hiding key. E.Data Decryption Decrypt Image: The image is decrypted using the encryption key used for encryption of the image. by using the encryption key a user can only access to the image Content[6]. De-embed Data: The data is extracted using the data hiding key used for the hiding the data into the image. by using the data

hiding a user can access only to the data within the encrypted image. Decrypt image and de-embed data: A user who has the both encryption key and data hiding key can access to the image and to the data hidden within the

A.Advance Encryption Standard AES is based on a design principle known as a Substitution permutation network. It is fast in both software and hardware. Unlike its predecessor, DES, AES does not use a Feistelnetwork.AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The block size has a maximum of 256 bits, but the key size has no theoretical maximum.AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field.The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. [5]Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. •KeyExpansion—round keys are derived from the cipher key using Rijndael's key schedule • Initial Round •AddRoundKey—each byte of the state is combined with the round key using bitwise xor• Rounds ¬ Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup.

¬ Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps. ¬Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.¬AddRoundKey B. Color histogram Techniques In image processing and photography, a color histogram is a representation of the distribution of colors in an image. For digital images, a color histogram represents the number of pixels that have colors in each of a fixed list of color ranges, that span the image's color space, the set of all possible colors. The color histogram can be built for any kind of color space, although the term is more often used for three-dimensional spaces like RGB or HSV. For monochromatic images, the term intensity histogram may be used instead. For multispectral images, where each pixel is represented by an arbitrary number of measurements (for example, beyond the three measurements in RGB), the color histogram is N-dimensional, with N being the number of

measurements taken. Each measurement has its own wavelength range of the light spectrum, some of which may be outside the visible spectrum. If the set of possible color values is sufficiently small, each of those colors may be placed on a range by itself; then the histogram is merely the count of pixels that have each possible color. Most often, the space is divided into an appropriate number of ranges, often arranged as a regular grid, each containing many similar color values. The color histogram may also be represented and displayed as a smooth function defined over the color space that approximates the pixel counts. The least significant bits have the useful property of changing rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). By contrast, the three most significant bits stay unchanged (000to000).Least significant bits are frequently employed in pseudorandom number generators, hash functionsandchecksums.LSB, in all capitals, can also stand for “Least Significant Byte”. The meaning is parallel to the above: it is the byte (or octet) in that position of a multi-byte number which has the least potential value in Steganography a message might be hidden or encrypt with in in an image by changing least significant bit to be the message bits then the image can be transmitted through network.lsb based Steganography is perhaps the most simple and straight forward approach .in this will only affect each pixel by +\-1, if at all ,it is generally assumed with good reason that degradation caused by this embedding process would perceptually transparent. hence there are number of lsb based Steganography techniques in the passive warden model as it difficult to differentiate cover-image from stegoimages ,given the small changes that have been made

CONCLUSION A novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and dataextraction/image-recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a datahiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional

data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of theencrypted image containing embedded data. However, the lossy compression method compatible with encrypted images generated by pixel permutation is not suitable here since the encryption isperformed by bitXOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation.

REFERENCES

[1] 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.

[2] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding (IH'2011), LNCS 6958, 2011, pp. 255–269, Springer-Verlag.

[3] 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.

[4] 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.

[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]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.

[7] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol.89, pp. 1129–1143, 2009.

[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] J.Mielikainen. LSB matching revisited. IEEE Signal Processing Letters, 13(5):285–287,2006.

[10] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su. Reversible data hiding. IEEE Trans. Circuits Syst.Video Technol., 16(3):354–362, 2006.

[11] S. Pereira and T. Pun. Robust template matching for affine resistant image watermarks.IEEE Trans. Image Process., 9:1123–1129, 2000.

[12] C.-M. Pun. A novel DFT-based digital watermarking system for images. Proc. SignalProcessing, 2, 2006.

[13] J. Tian. Reversible data embedding using a difference expansion. IEEE Trans. CircuitsSyst. Video Technol., 13(8):890–896, 2003.

[14] S.-H.Wang and Y.-P. Lin.Wavelet tree quantization for copyright protection watermarking.IEEE Trans. Image Process., 13:154–165, 2004.

[15] Y.N. Wang and A. Pearmain. Blind image data hiding based on self reference. Pattern Recognition Lett., 25:1681–1689, 2004.

[16] Y.P. Wang, M.-J.Chen, and P.-Y. Cheng, Robust image watermark with wavelet transform and spread spectrum techniques. In Proceedings Thirty-Fourth Asilomar Conference on Signals, Systems and Computers, Vol. 2, pages 1846–1850, 20009

[17] D.C. Wu and W.H. Tsai. A steganographic method for images by pixel-value differencing Pattern Recognition Lett., 24(9–10):1613– 1626, 2010.

[18] 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. Proc. Inst. Elect. Eng., Vis.Images Signal Process., 152(5):611–615, 2009.

[19] C.-H. Yang, C.-Y.Weng, S.-J.Wang, and H.-M. Sun. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans. Information Forensics and Security, 3(3), 2008.