International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 05, May-2015

An Algorithm Extracting Hidden Data from Encrypted Images using IWT

Mr. Nitin Laxman Shelake
Department of Computer Engineering
SND college of Engg. & Research Center,
Yeola(Nashik),India

Prof. Santosh R. Durugkar
Department of Computer Engineering
SND college of Engg. & Research Center,
Yeola(Nashik),India

***Abstract*—Reversible data hiding technique in which the hidden data property is maintained even after processing on the image. The original cover image remains same after processing on the embedded image, original data is obtained. The image is used to embed additional information in the encrypted images, applies in many fields of security which can be recoverable with original media and the hided data without loss. Some previous methods embed data reversible vacating room from the encrypted images, which matter to error on data extraction and/or image restoration. This system proposes a reversible data hiding technique which work is separable; the receiver can extract embedded data. If a system for lossless compression of images applies a recover step, this step must map integer input values to integer output values. This can be achieved using the integer wavelet transform. This proposed system can achieve the excellent reversibility, that is, data extraction and same image quality. This system is better to handle secret communication in open environment like internet through which we can send embedded images having encrypted information.**

Keywords—Reversible Data Hiding, Image Encryption, Data Protection, Integer wavelength Transform

I. INTRODUCTION

This Data hiding using Reversible data hiding technique. Is a technique which hides data behind the image and an original data are retrieved after the processing on the encrypted image. [1]; There is a lot of research done on signal processing of encrypted images. Hiding data and maintains the privacy of the data is very useful. However, in some situations that a content holder does not trust the processing service provider, it is thus able to keep the data unrevealed but in encrypted form. For instance, when the secret data to be transmitted are encrypted, a channel provider without knowing anything of the cryptographic key may try to compress the encrypted data due to the limited resources. [8] Image security has becomes increasingly important for many applications mostly related to internet e.g. confidential transmission, military and medical application purpose.

The encryption or data hiding algorithm can be used to protect to multimedia data. There was a problem faced to try to combine compression, encryption and data hiding in a single step. For example, solutions were proposed to combine image encryption and compression [9]. Two groups of technologies have been developed to solve. First technique is based on content protection through encryption. There are several approaches to encrypt [8] binary images or gray level images. By wishing to remove the embedded data before the image decryption, a new idea is to apply reversible data hiding algorithm on encrypted images [8]. Recent reversible data hiding methods have been recommended with high capacity, but these methods are not applicable on encrypted images.

II. EASE OF USE

A. *Reversible Data Hiding:*

As data hiding is a process of hiding data[4] behind the cover media. That is, the data hiding process has two sets of data, one set of the embedded data and another set of the cover media data. [2] The association between these two sets of data characterizes different applications. For instances, in covert communications the hidden data may often be relevant to the cover media. In verification however the embedded data are closely related to the cover media. [3] In most cases of data hiding the cover media experiences some distortion due to data hiding and inverting back to the original media is not possible. That is some stable distortion has occurred to the cover media even after the hidden data have been extracted out. It is used in medical and law forensics was data secrecy has to maintain

B. *Reserving room before Encryption:*

Define Lossless vacating room from the encrypted images is relatively difficult and inefficient, so reverse order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH tasks in encrypted images would be more natural and much at ease which leads us to the novel framework, “reserving room before encryption (RRBE)”. [1] The data removal and image recovery are identical to that of Framework VRAE. Standard RDH algorithms are ideal for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. [1] This is because in this new framework, follow the customary idea that first lossless compresses the redundant image content (e.g., using admirable RDH techniques) and then encrypts it with respect to protecting privacy. Next elaborate a practical method based on the Framework “RRBE”, which primarily consists of four phases: generation of encrypted image, data hiding in encrypted image, data extraction and image recovery. [8]

III. RELATED WORK

The first technique was proposed by Honsinger et al. [15] in 2001 which used modulo-256 arithmetic to attain reversibility. The embedding formula is ( )mod 256 w I = I +W in which I denotes the original image and Iw the steno-image and the watermark W =W(H(I),k) , where H(I) denotes the hash function and k the secret key. The usage of modulus 256 additions, the over/underflow is prevented and reversibility is achieved. Basically the reversible data hiding methods developing till date can be classified into two main types based on the embedding domain. The first type applies data embedding in the spatial domain, with relatively low capacity, while the other type utilizes the coefficients in the transform areas, such as the integer DCT and the integer wavelet transform domains to hide the data [14].

In 2006, Ni et al. [12] proposed a reversible data hiding method established on histogram shifting. The scheme used the zero point and peak point of an image histogram to hide message and achieved reversibility. The arrangement was quite simple and caused only slight distortion with low complexity. However, the experimental results demonstrate that its biggest hiding capacity is only about 5000 bits when the test image is 8-bit gray scale and of size 512×512.

In 2008, Lin_et al. [13] proposed a reversible data hiding based on histogram alteration of difference image generated from the linear prediction scheme. Besides that they also offered to apply the algorithm multiple times in order to achieve high embedding capacity. It does not matter whether specialists hide embedded messages in the spatial, frequency or compression domains. A common approach in reversible data hiding is to define a free space in an image first, also called the hiding area and then hide the embedded message in that area. To hide a more payload in an image and maintain the highest possible image quality of a marked image at the same time, inspired by Ni et al.'s scheme [10], we explore the peak point of the histogram in pixel differences in an image, then slightly modify the pixel values to hide the embedded message. This paper shows scheme uses a multilevel hiding strategy to provide large hiding capacity while keeping distortion low. Histogram is nothing but a graph that shows frequency of incidence of data. Histograms have much use in image processing, which we are going to discuss one user here which is called histogram shifting[5]. In which space is saved for data embedding by shifting the bins of histogram of gray values. The state-of-art methods usually combined DE or HS to residuals of the image, eg. The predicted errors, to achive better performance.

In Xuan ct al. [13] propose a lossless data hiding having large capacity based on integer wavelet transform. It hides authentication information and bookkeeping data into a middle bit-plane of integer wavelet coefficients in high frequency sub-bands. The histogram modification or integer modulo addition is used to prevent gray scale overflowing during data embedding. The method uses second-generation wavelet transform IWT [14].

The authors find more bias between 1s and 0s starting from 2^{nd} bit-plane to higher bit-planes of IWT coefficients. To make the watermarked image perceptually as same as the original image and to have high PSNR they tell to embed information into middle bit-plane and in the high frequency sub-bands respectively. To compress it they use arithmetic coding from [16]. The watermark payload concatenated with compressed data is embedded with a secret key. In extraction phase, the watermark (say, hash of original image) is extracted and the original image is reconstructed in the opposite manner. To prevent the gray-scale overflow either histogram modification or gray scale modification is used as pre-processing and post-processing during embedding and extraction phases respectively.

IV. SYSTEM OVERVIEW

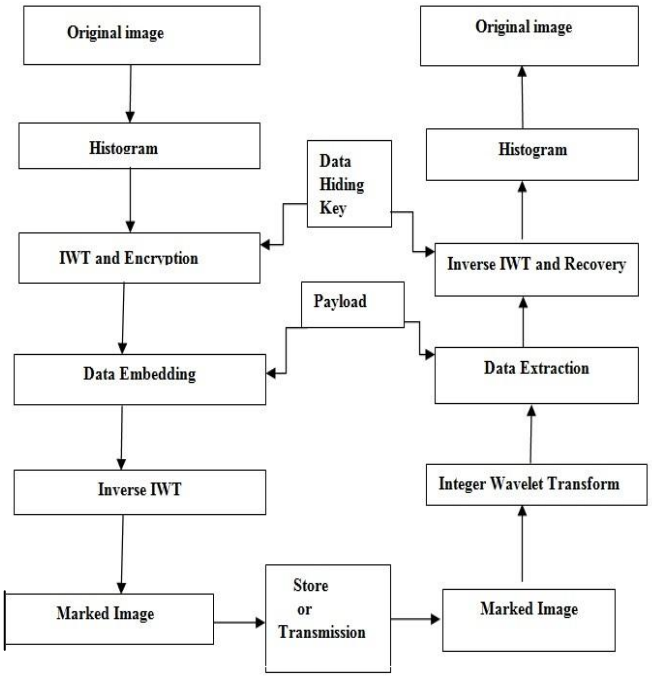

Figure:-1 Block Diagram for Data Embedding and Data Extraction

3.1 Integer Wavelet Transform (IWT):-

To recover the original image lossless, reversible wavelet transform should be used. Hence we employ the integer wavelet transform which maps integer to integer [14] and can reconstruct Although various wavelet families can be applied to our reversible embedding scheme, through experimental assessment study we have discovered that CDF (2, 2) is better than other wavelet families in terms of high embedding capacity and visual quality of marked images. CDF (2, 2) format has also been accepted by JPEG2000 standard.

Distribution of IWT [13]coefficients in High Frequency Sub bands and Selection of function for most of images, the scattering of high frequency coefficients of integer wavelet transform obeys in general a Laplacian-like distribution. The following two structures exist in the distribution. (a) Most high frequency integer wavelet transform coefficients are very small in extent. It is then convenient to select the compression function. For example the linear function eq (1)

$$f(x) = x$$

Can be considered as compression function since even though y′ is twice the x value, it is still in the range of x.

(b) Although most of high frequency IWT coefficients are small in amount, there are still some IWT coefficients having large magnitude. For these big coefficients, compression function selection should consider the limit of condition. In this case, the linear function from Eq (1) is no longer suitable to serve as a compression function. Considering the above two conditions, we propose to adopt the following piecewise linear function as the compression function.

$$C(x) = \begin{cases} x, |x| < T \\ sign(x) \cdot (\frac{|x| - T}{2} + T), |x| \geq T \end{cases}$$

where T is a pre-defined threshold. C x( ) is depicted below in Figure 2

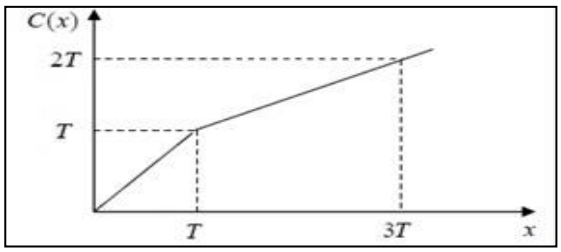

Figure:-2 Compression function C(x)

As discussed above, in actual realization, however, we have to adopt the compress function in quantized version,

It can be derived from the above equation that when x ≥ T , x and (x +1) (or(x −1)) are compressed to correspond to a same y value. Hence according to the previous discussion, x and (x +1) (or (x −1)) are need to be recoded, the recording data need to be embedded as overhead into the wavelet coefficients. From the above discussion, T is a critical value. hen T is small, the coefficients alterations are small and worthy visual quality of marked image are achieved. When T is large, a larger payload can be achieved. In the actual embedding, we select the T value allowing to the payload [14].

3.2 Histogram Shifting :

For a given image, after data are embedded into some high frequency IWT coefficients,[13] it is possible to cause overflow and/or underflow, which means that after inverse integer wavelet transform[11,14] the grayscale values of some pixels in the marked image may exceed the higher bound (255 for an eight-bit grayscale image) and/or the lower bound (0 for an eight-bit grayscale image). In order to prevent the overflow and underflow, we implement histogram modification to narrow the histogram from both sides. The bookkeeping data generated in histogram modification need to be embedded into image as a part of overhead data, which will be used late in the retrieval of the original image.

3.3 Data Embedding:

The processing pair of compression and expansion is a technique utilized to implement no uniform quantization[10] in speech communications in order to achieve high signal noise ratio. This has been in depth presented in many digital communications texts, say, in [6]. Exactly, this procedure first wrappings a signal and then expands it. Uniform quantization is supported out after the compression and before the enlargement.

3.4 Algorithm for proposed system:

The following are the algorithmic steps for proposed system

Step 1: Input: Let {I} be the image to be input.
Step 2: Divide image into different ubbands.
Step 3: For each pixel I in image
Step 4: Calculate avg = (r+g+b)/3
Step 5: Apply reversible wavelet transform
Step 6: Generate Histogram
Step 7: Construct original signal without any distortion IWT
Step 8: Data Compression
Step 9: Data embedding
Step 10: Inverse integer wavelet transform
Step 11: Marked image
Step 12: Maintaining high PSNR

3. 5 State Diagram :-

Let,
S0= Apply reversible wavelet transform.
S1= Generate Histogram.
S2= Construct original signal without any distortion IWT.
S3= Data Compression.
S4= Data embedding.
S5= Inverse integer wavelet transform
S6= Marked Image.
S7= Maintaining high PSNR.

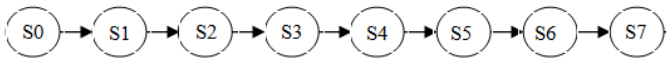

Fig. 4 state diagram for system

VI. Experimental Results and Analysis

We applied the recommended reversible data hiding algorithm to some frequently used images. Tables 1, 2, 3, and 4 enclose the experimental results on four grayscale level images, Lena, Baboon, Barbara and Goldhill of size 512×512 shown in Figure 5. The data in these tables indicate that the proposed reversible data hiding algorithm can embed a large payload, while maintain the high PSNR (peak signal-to-noise-ratio) of the marked image versus the original image.

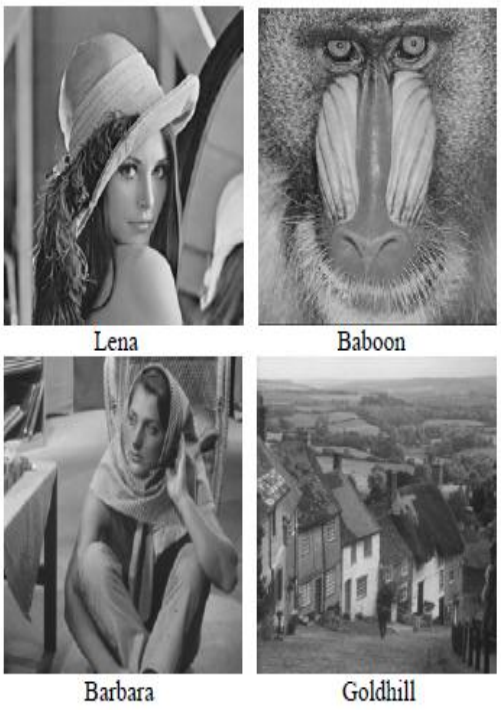

Fig. 5. Lena,Baboon,Barbara,Goldhill

Table 1. PSNR vs. payload for Lena image

payload (bpp)	0.1	0.2	0.3	0.4	0.6	0.7
PSNR (DB)	51.53	48.23	46.04	44.28	41.43	39.48

Table 2. PSNR vs. payload for Baboon image

payload (bpp)	0.1	0.2	0.3	0.4	0.5
PSNR (DB)	45.45	41.66	38.42	35.61	33.51

Table 3. PSNR vs. payload for Barbara image

payload (bpp)	0.1	0.2	0.3	0.4	0.5	0.6
PSNR (DB)	51.47	48.84	46.70	44.33	42.13	38.77

Table 4. PSNR vs. payload for Goldhill image

payload (bpp)	0.1	0.2	0.3	0.4	0.5	0.6
PSNR (DB)	49.85	46.74	44.37	42.40	40.36	38.68

We should point out that this proposed can be applied successively for a few times on the same image which means we can remain to embed data on the marked image. Since we embed data in three extraordinary frequency subbands of IWT, the theoretical upper bound for data embedding is 0.75 bpp each time. Results reported in Tables 1, 2, 3, and 4 are the first time embedding. For most of images, however, it can embed data at 1.3 bpp after three times data embedding. After that, if we further embed data on the marked image, the payload will increase very slowly while the visual quality drops severely as shown in Figure 6.

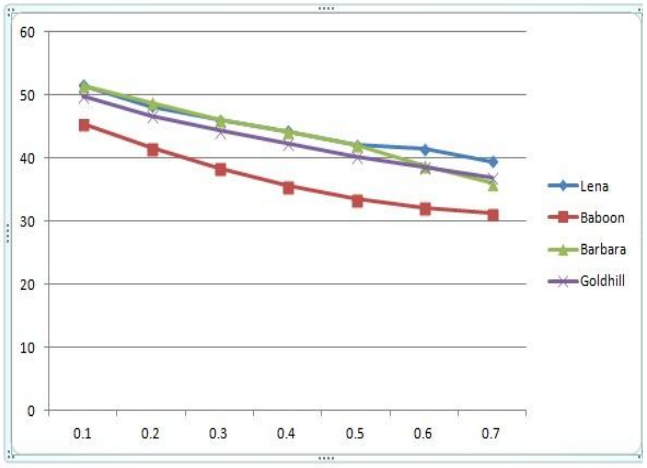

Fig. 6-Result of psnr and payload

V. CONCLUSION AND FUTURE SCOPE

This proposed method in encrypted images is a new topic drawing attention because of the privacy-preserving requirements form cloud data management. This system has achieved more payload capacity, Ensuring the correct data-extraction, perfect image recovery and prevention of image from external attacks. Also Less degradation in Image quality during Recovery and helpful to image denoising.

VI. ACKNOWLEDGMENT

I am very much thankful to my respected project guide and Head of Dept. Prof. Durugkar S. R. for his ideas and help, proved to be valuable and helpful during the creation of this paper and set me in the right path. I am also very much thankful to PG Co-ordinator Prof. Shaikh I. R. for helping us while selecting and preparing for paper work. I would also like to thank all the faculties who have learned all the major concepts that were involved in the understanding of techniques behind my seminar. Lastly, I am thankful to my friends who shared their knowledge in this field with me.

REFERENCES

(1) Kede Ma, Weiming Zhang, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" IEEE Transactions On Information Forensics And Security, Vol. 8, No. 3, March 2013
(2) Zhicheng Ni, Yun-Qing Shi, "Reversible Data Hiding" IEEE Transactions On Circuits And Systems For Video Technology, March 2006.
(3) 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,
(4) Mohammad Ali Alavianmehr, Mehdi Rezaei Mohammad Sadesgh Helfroush, "A Semi-Fragile Lossless Data Hiding Scheme Based on Multi-level Histogram Shift in Image Integer Wavelet Transform Domain.
(5) P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme Using predictive coding and histogram shifting," Signal Process. Vol. 89, 2009.
(6) X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Let's., vol. 18, no. 4, Apr. 2011.
(7) J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

(8) 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.
(9) X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
(10) W. Du and M. J. Attalla, "Privacy-preserving cooperative scientific computations," in Proc. 14th IEEE Computer Security Foundations Workshop, Nova Scotia, Canada, Jun. 11–13, 2001, pp. 273–282.
(11) J. Tian, "Wavelet-based reversible watermarking for authentication," in Security and Watermarking of Multimedia Contents IV—Proc. SPIE, E. J. Delp III and P. W. Wong, Eds., Jan. 2002, vol. 4675, pp. 679–690.
(12) M. Fujiyoshi and H. Kiya, "Reversible Information hiding and its Application to image authentication," in Multimedia Information Hiding Technologies and Methodologies for Controlling Data, K. Kondo, Ed.IGI Global, Oct. 2012, pp.238–257.
(13) Xuan, G., Zhu, J., Chen, J., Shi, Y. Q., Ni, Z., Su, W.: Distortionless Data Hiding Based on Integer Wavelet Transform. In: IEE Electronics Letters, December (2002) 1646-1648.
(14) Calderbank, A. R., Daubechies, I., Sweldens, W., Yeo, B.-L.: Wavelet Transforms that Map Integers to Integers. In: Applied and Computational Harmonic Analysis, July (1998) 332–369.
(15) W. Bender, D. Gruhl, N. Morioto and A. Lu, "Techniques for data hiding," International Business Machines Corporation System Journal, vol.35, pp. 13-336, 1996.
(16) Y. Q. Shi. And H. Sum, "Image and Video compression for Multimedia Engineering", Boca Raton, FL:CRC,1999