ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 7, Issue 4, April 2018

INTEGER WAVELET TRANSFORM AND HISTOGRAM SHIFTING FOR HIGH DEFINED IMAGES BY DATA HIDING

Sathyabhama.B, Preethi.V, Shalini.V, Sandhya.C, Yuvarani.T

Panimalar Engineering College, Chennai 600123

ABSTRACT

A reversible data hiding (RDH) scheme for encrypted digital images using integer wavelet transform, histogram shifting and orthogonal decomposition is presented. We use the integer lifting scheme based on wavelet transform in this framework as it is required to reconstruct the original image. The advantage of this scheme is to provide Laplacian-like distribution of integer wavelet high-frequency coefficients in high frequency sub-bands and the independence of orthogonal coefficients to facilitate data hiding operation in encrypted domain, and to keep the process of reversibility in a correct manner. The demonstration of experimental result states that this scheme outperforms all of other existing RDH schemes in encrypted domain in higher PSNR terms at the same amount of payload. Compared with the state-of-the-arts, the proposed scheme can be applied with higher embedding rate to all natural images.

Keywords: Reversible data hiding, Integer Wavelet Transform, Cryptography and Steganography, Histogram shifting.

1. Introduction

Reversible Data Hiding (RDH) method is able to erase completely the distortion caused by embedding of data after the hidden data have been extracted out. This major technique is widely used in remote sensing imagery, law forensics, medical imagery, where no distortion of the original cover is desired [4].In recent years, many RDH techniques have been proposed which are mainly based on the following three strategies: lossless compression [1], Difference Expansion (DE) [7] and Histogram Shift (HS) [4] approaches. Almost all RDH algorithms comprises of two steps. The first step generally creates a host sequence with small entropy, e.g., the host has a sharp histogram which usually can be obtained or realized by using Prediction Errors (PE) method with the sorting technique [6] or the selection of pixel. The second step embeds the additional message bits into the host sequence in a reversible manner. In the increasing demand of privacy protection, signal processing in encrypted domain has attracted considerable research interests. With regard to providing confidentiality for multimedia content, encryption is an effective and best approach as it can protect multimedia information from illegal access by

transforming the original data information into encrypted content during the transmission processes, storage, etc. Since this is well-known, partial encryption is an approach to reduce the computational resources for huge volumes of multimedia data in low power network [5], [3]. Hence, current image encryption mainly focuses on partial encryption. However, in some cases, a content owner does not want the service provider access the content of original multimedia as they may not trust the processing service provider, such as Cloud-based storage service. Before submitting, the content owner will encrypt the image [10]; [9]. For authentication, notation and copyright protection, the service provider would embed some additional messages into the encrypted image. Therefore, many schemes of RDH in encrypted domain have been proposed recently. Zhang proposed a least significant bits (LSBs) modification scheme to achieve the RDH for encrypted image [13], [2] Zhang's method was improved via using side match technique. And as preprocessing, this scheme chooses a better metric to measure the block smoothness. In order to data extraction, these two methods need to rely on decrypted images. However, the decrypted images may not be provided or be unknown in order to maintain the confidentiality of images. To separate data extraction from encrypted image, Zhang introduced a method to separate, in which a receiver having the data hiding key can extract the additional data and a receiver having the encrypted key can decrypt received data to obtain or get an image similar to the original image. Anyhow, these methods can only achieve low capacity of embedding or generate marked image with low or poor quality in the case of high embedding capacity. Zhang et al. proposed a method of improved reversibility.

2. Literature survey

In this technique, embedding space is vacated firstly by shifting the histogram of estimating errors of some pixels (I_a) chosen by only when neighborhood of these pixels includes atleast T pixels in E (E is a set of estimating values, T is a threshold ($1<=T<=8$)). Hence, the method is also called as reserving room before encryption (RRBE). This kind of method for encoding generally comprises of three steps. The first step creates or generates a host sequence with reserving room. Secondly, encrypts the host sequence. Finally, the third step is to reversibly embeds the additional message bits into the encrypted sequence. In the phase of decoding, the data hider can extract the additional bits by a hidden key. The operator for data decryption can decrypt the encrypted-marked data by a decrypted

key. However, this technique is not applicable to some images where no enough pixels can be selected to form vacating room, i.e., rather the data embedding rate is limited. Additionally, this method would cause high computation complexity due to the specific or certain arrangements for embedding space. Moreover, in RDH schemes for encrypted images, encryption of an image should be arranged to the content owner. Meanwhile, embedding of data is supposed to be accomplished by the service provider [8]. Therefore, RDH scheme in encrypted domain needs to keep independence between the steps of extraction and decryption. Based on the above analysis of the method, this paper proposes an integer wavelet transform based scheme for reversible data hiding in encrypted images.

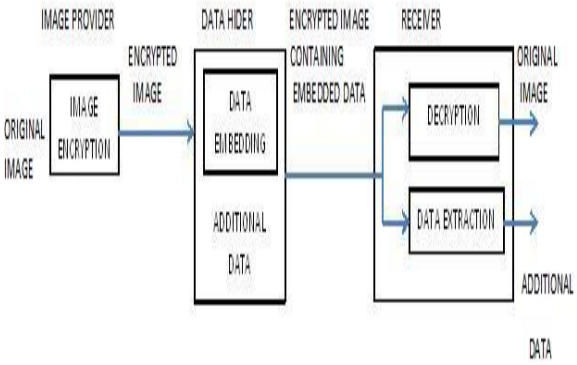


fig2 sketch of lossless data hiding scheme for public key encryption.

The commonly used method of hiding data is covering the secret data by adding a key to it. In the lossless and reversible data hiding three types of schemes are used lossless, reversible and combined data hiding scheme. In the lossless scheme, cipher text pixels are converted into new pixel in the new pixel we can add additional data in it. To do this process multi-layer wet paper coding is used. After loss less scheme, reversible scheme is done in which image is shrink, this is done before the encryption process by doing so overlap of image will not occur. The last process is combined data hiding scheme in this we can extract the embedded data before decryption and the original image after decryption using a public key. By using public key anyone can extract the hided image and so a new technique is introduced for hiding a data in very well secured manner. For secured hiding we use integer wavelet transform scheme.

3. Proposed method

In this section, firstly we introduce integer wavelet transform (IWT) and encryption

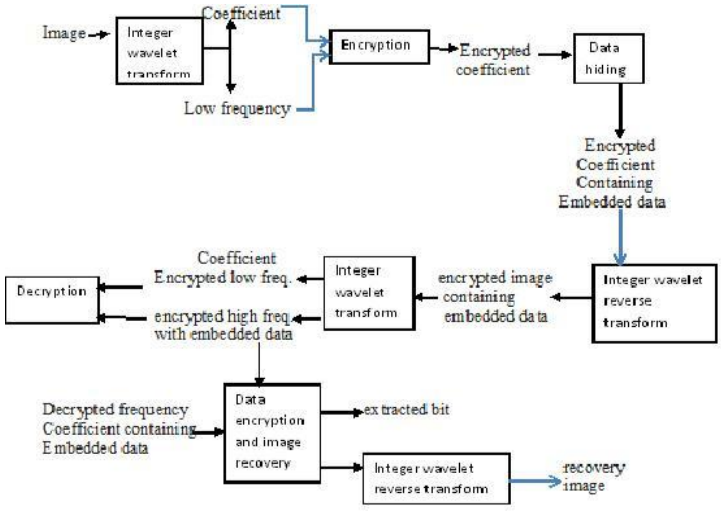


Fig 1 shows the framework of proposed method

method used in the paper. Then we introduce algorithm of data hiding to embed additional data into the encrypted image. In this way, the additional data is embedded in encrypted domain. Firstly, an image is processed using the integer wavelet transform. Secondly all frequency coefficients are encrypted. In the third step, with additional data the encrypted frequency are embedded. To obtain an encrypted image containing embedded data, integer wavelet reverse transform is processed on encrypted coefficients containing embedded data. Decrypted image containing embedded data is obtained in the decryption phase. From the encrypted high frequency coefficients containing embedded data, the embedded data is extracted directly in the data extraction phase and encrypted image without embedded data is also obtained. The extraction of embedded data from decrypted image containing embedded data is another way of extracting embedded data. At last recovered image is obtained.

The independence of orthogonal coefficients can facilitate data hiding in encrypted domain in a transformation matrix and the reversibility is kept.

3.1 Integer wavelet transform

Based on the wavelet transform in this frame work we use integer lifting scheme because to reconstruct the original image it is needed. CDF (2, 2) integer wavelet transform is adopted for the experiment [12], [11]. We have four sub-bands after the IWT.

A high frequency coefficient is denoted as X and the other coefficients are denoted as X'. Transformation matrix is denoted as $B = (b_1, b_2, b_n)$ of size n x n which satisfies the following equations.

$$b^T_i \cdot b_j = 0 \text{ if } i = j$$

$$b^T_i \cdot b_j = 0 \text{ otherwise } i, j = 1, 2, n \quad (1)$$

Where $b_i=(b_{i1}, b_{i2} \ldots b_{in})^T$ is an n-dimensional column vector in B. X can be represented as $X = B \cdot Y$ or $Y = B\text{-}1$ using orthogonal decomposition based on B, where Y is a set of the orthogonal coefficients. The matrix B and vector Y can be divided into two sub-matrixes and sub-vectors respectively, i.e., $B = (R, S)$ and $Y = (Y_1, Y_2)^T$, thus R and S can be expressed as $R = (b_1, b_2, \ldots, b_m)$ and $S = (b_{m+1}, b_{m+2}, \ldots, b_n)$. Therefore, Y_1 and Y_2 are controlled by R and S separately. X can be described as follows.

$$X = R \cdot Y_1 + S \cdot Y_2 \quad (2)$$

$Y_1=(R^T \cdot R)^{-1} \cdot R^T \cdot X$

Similarly, multiplying $(S^T \cdot S)^{-1} \cdot S^T$ by Eq. (2), we can obtain $Y_2=(S^T \cdot S)^{-1} \cdot S^T \cdot X$

Therefore, according to Eqs. (1)– (2), we can obtain Eq. 3 $Y_1=(R^T \cdot R)^{-1} \cdot R^T X$ and $Y_2=(S^T \cdot S)^{-1} \cdot S^T \cdot X$

Then, substituting $Y_1=(R^T \cdot R)^{-1} \cdot R^T \cdot X$ into Eq. (2), we can obtain Eq.(4).

$$S \cdot Y_2 = X - R \cdot (R^T \cdot R)^{-1} \cdot R^T \cdot X. \quad (4)$$

3.2Decryption and data extraction procedures:

Firstly, we separate X_{eh} from $X`_e||X_{eh.}$ by wavelets transform. Then, the embedded data is extracted from X_{eh} by data hider. At the same time, the data decryption operator decrypts X_{eh} and X'_e with a decrypted key. There are two scenarios considered: Data extraction before image decryption and image decryption before data extraction.

Data extraction before image decryption:

In this scheme, for the data hider, S and X_{eh} are known. Accordingly, the data hider can get $Y_{2h}$from the encrypted high frequency coefficients containing embedded data, X_{eh}. The procedures are as follows,

$$Y_{2h}= (S^T\cdot S)^{-1}\cdot S^T\cdot X_{eh}$$

Here we obtain Y_{2h}, and then the embedded data can be extracted from Y_{2h} with extraction procedures .Similarly, Y_{2h} can also be recovered to Y_2.

Image decryption before data extraction:

For the data decryption operator, R, X_{eh} and $X`_e$ are known. The procedure is as follows:

$Y_{1e}=(R^T\cdot R)^{-1}\cdot R^T\cdot X_{eh}$,

$Y_1 = Dec\ (Y_{1e}, K) = Dec\ ((R^T\cdot R)^{-1}\cdot R^T\cdot X_{eh}, K)$

And $X` = Dec(\acute{X}\ e, K)$

where $Dec(\cdot, \cdot)$is a decryption function.

Based on the above analysis, the R can be used as control codes of encryption and S can be used as data hiding, which keep the independence between data extraction and image decryption.

3.3 Analysis:

From the above construction of proposed scheme, we can obtain that the security of proposed scheme relies critically on the security of encryption and data embedding techniques used in our construction, and the security of orthogonal coefficients. The encryption and data embedding techniques used, such as stream cipher and histogram shifting, are mature and well-studied which is believed to be secured, if properly used.

In this proposed scheme, the Y_2 coefficients are unencrypted. There is a possibility that the attackers may use the unencrypted data as a security leak to attack the protected information. However, the degree to which the unencrypted data may reveal the protected information needs to be assessed. Assume the protected data is I,I can be expressed as follows

$$I = f\ (X, X') = f_1(X) + f_2(X')$$

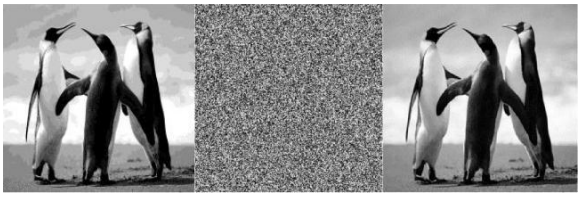
Where $fi\ (\cdot, \cdot)$ $(i = 1, 2)$ is a linear function that is determined by an image encoding algorithm, X is selected host vector set, X' is other data. Thus, I_e, the encrypted image is given as follows,

$I_e = f_2(X'_e) + f_1(X_e) = f_2(X'_e) + f_1(R\cdot Y_{1e}) + f_1(S\cdot Y_2)$

In I_e, only $f_1(S\cdot Y_2)$ is unencrypted, thus it is the only term that might lead to some information leakage. However, if X is properly defined, R and S are appropriately selected, and then the potential information leakage can be controlled within an acceptable range.

4. Experimental results:

Our proposed scheme is compared with other reversible data hiding schemes in encrypted domain. Penguin image is taken as standard test image with size 1024 x 768 shown in fig 4(a) is adopted to demonstrate the feasibility of the proposed method. To facilitate, the implementation of the proposed scheme, Walsh Transform is chosen to generate a transformation matrix B with the size of 8×8. And the size of R and S are the same, 8×4. High frequency coefficients are arranged to form many 8x8 blocks. MATLAB is used for simulations. Stream cipher is used as encryption method. Pseudo-random bits $r_k\ (i, j)$ is generated by an encryption key using a standard stream cipher. Pseudo-random bits generated are used to encrypt $Y1$ and $\acute{}X$ by exclusive-or operation.

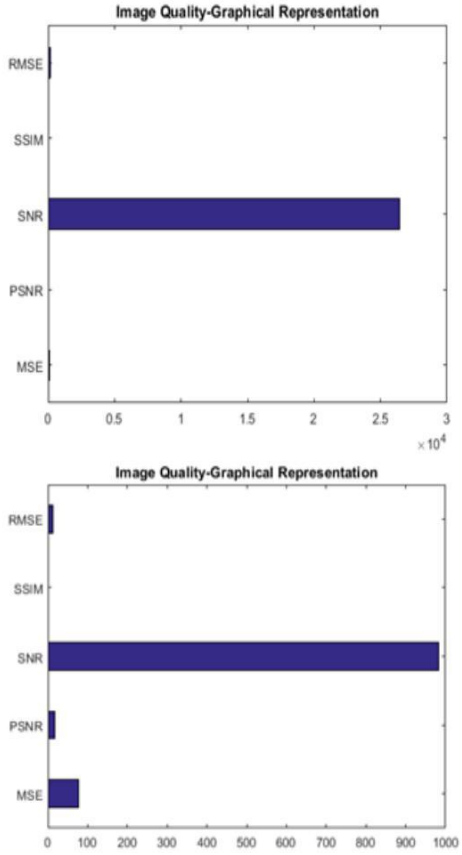


(a) (b) (c)

Fig 4 (a) original penguin image (b) encrypted image and (c) marked and decrypted penguin image with PSNR = 16.9089dB

When the graph is plotted we get the following values:

CRITERIA	ORIGINAL IMAGE	RECOVERED ORIGINAL IMAGE
RMSE	12.6	162.591
SSIM	0.27	0.0017354
SNR	986.232	1435.7
PSNR	77.313	16.9089
MSE	77.313	76.8381



5 Discussion and conclusion

In this paper, a novel scheme for reversible data hiding in encrypted image has been reported. This paper is based on Integer Wavelet Transformation (IWT), histogram shifting and orthogonal decomposition. In the proposed scheme, laplacian-like

distribution has integer wavelet high-frequency coefficients and the histogram shifting technique can be well carried out in these coefficients. The data hiding operation in encrypted domain is facilitated due to the independence of orthogonal coefficients and keep the reversibility.

In terms of higher PSNR at the same amount of payload, we get the experimental results which show that is has superior performance over the current state of the art [14] [13]. And the penguin image has wider applicability therefore; the proposed scheme can embed much more data into the image. In this scheme, various data embedding methods can also be applied. Proposing a novel scheme for reversible data hiding is the aim of this paper. As for the other data embedding and encryption methods, we will discuss these methods and explore a better performance method in future.

REFERENCES

[1] Fridrich, J., & Goljan, M. (2002). Lossless data embedding for all image formats. In *SPIE proceedings of Photonics west, electronic imaging, security and watermarking of multimedia contents* (Vol. 4675, pp.572–583). San Jose.

[2] Hong, W., Chen, T. S., & Wu, H. Y. (2012). An improved reversible data hiding in encrypted images using side match. *IEEE Signal Processing Letters*, *19*(4), 199–202.

[3] Korshunov, P., & Ebrahimi, T. (2014). Scrambling-based tool for secure protection of JPEG images. In *2014IEEE international conference on image processing (ICIP)* (pp. 3423–3425). IEEE.

[4] Ni, Z. C., Shi, Y. Q., Ansari, N., & Su, W. (2006). Reversible data hiding. *IEEE Transactions on Circuits and Systems for Video Technology*, *16*(3), 354–362.

[5] Puech,W.,& Rodrigues, J. M. (2005). Crypto-compression of medical images by selective encryption of DCT. In *2005 13th European signal processing conference* (pp. 1–4). IEEE.

[6] Sachnev, V., Kim, H. J., Nam, J., Suresh, S., & Shi, Y. Q. (2009). Reversible watermarking algorithm using sorting and prediction. *IEEE Transactions on Circuits and Systems for Video Technology*, *19*(7), 989–999.

[7] Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE Transactions on Circuits and Systems for Video Technology*, *13*(8), 890–896.

[8] Wu, X.,&Sun,W. (2014).High-capacity reversible data hiding in encrypted images by prediction error. *Signal Processing*, *104*, 387–400.

[9] Xia, Z., Wang, X., Zhang, L., Qin, Z., Sun, X., & Ren, K. (2016). A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. *IEEE Transactions on Information Forensics and Security*,.

[10] Xiong, L., Xu, Z., & Xu, Y. (2015). A secure re-encryption scheme for data services in a cloud computing environment. *Concurrency and Computation: Practice and Experience*, *27*(12), 4573–4585.

[11] Xuan, G.,Yao, Q.,Yang, C.,Gao, J., Chai, P., Shi,Y. Q.,&Ni, Z. C. (2006).Lossless data hiding using histogram shifting method based on integer wavelets. In *2016 international workshop on digital watermarking (IWDW), lecture notes in computer science* (Vol. 4283, pp. 323–332). Berlin, Heidelberg: Springer.