JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

PUBLIC KEY CRYPTOGRAPHY ENABLES LOSSLESS AND REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES

[1] Syed Ceyana, [2] P.Venkata Sai,M.Tech
[1]M.Tech PG Scholar, [2]Asst.Professor
[1,2]Deptartment Of ECE,
[1,2] SKR College of Engineering and Technology,Konduru satram (v),Manubolu(m),SPSR Nellore(dt),Andhra Pradesh.

Abstract : For hiding secret data in digital images, large varieties of techniques are available, some are more complex than others. Public key cryptography has various useful applications and the technique employed depends on the requirements of the application to be designed for. Reversible data hiding is a type of data hiding techniques whereby the host image can be recovered exactly. Being lossless makes this technique suitable for medical and military applications. The ciphertext pixels are replaced with the additional data into new values to embed several ciphertext pixels by wet paper coding at multiple layer. From original image the embedded data can be extracted and the original image can be recovered from the decrypted image directly. The embedded data can directly be extracted from the encrypted domain. The decryption of original plaintext image doesn't affects data embedding operation. With the combined technique, before decryption a receiver may extract a part of embedded data, and recover the original plaintext image after decryption. A slight distortion is introduced due to the compatibility between the lossless and reversible schemes. The data embedding operations can be performed in the two manners simultaneously performed in an encrypted image and decrypted image.

Keywords: Image encryption, Lossless data hiding, Reversible data hiding, Public key encryption

I. Introduction

Encryption and information hiding are two viable methods for information security. The ciphertext pixels are replaced with additional data as new values are embed into various LSB-planes at multi-layer wet paper coding. Then, embedded data is extracted directly from the encrypted domain, and the decryption of original plaintext image is not affected by the data embedding operation. While the encryption procedures change over plaintext content into mixed up ciphertext, the information concealing strategies insert extra information into spread media by presenting slight alterations. In some mutilation unsuitable situations, information concealing can be performed with a lossless or reversible way. In spite of the fact that the expressions "lossless" and "reversible" have same which means in an arrangement of past references, we would recognize them in this work. Information hiding technique is lossless if the display of cover signal containing installed information is same as that of unique cover despite the fact that the spread information have been adjusted for information inserting. For instance, the pixels with the most utilized shading as a part of a palette picture are doled out to some unused shading lists for conveying the extra information, and these files are diverted to the most utilized shading. Thusly, despite the fact that the files of these pixels are modified, the genuine shades of the pixels are kept unaltered. Then again, we say an information concealing system is reversible if the first cover substance can be consummately recouped from the spread rendition containing installed information despite the fact that a slight bending has been presented in information implanting strategy. Various instruments, for example, distinction extension, histogram shift and lossless pressure, have been utilized to build up the reversible information concealing systems for computerized pictures. As of late, a few decent forecast methodologies and ideal move likelihood under payload-mutilation measure have been acquainted with enhance the execution of reversible information covering up.

1.2 Motivation of the Project

In Existing system there was problem of loss of data from the drawback of the existing system we got motivation.

1.3 Literature Survey

High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis: A lossless embedding technique is proposed as image histograms are analysed to identify the image types for different capacity. In embedding capacity estimation histogram maxima and minima techniques are used. Nowadays either lossy or lossless techniques are used for data embedding over images. Lossy techniques can allow large hiding capacity but host image cannot be recovered with high performance. In Some applications exact recovery of the host image is required, as in medical image patient data can be embedded without affecting actual image. The lossless data hiding techniques has to face from limited capacity as host image should kept personal. The proposed technique enables hiding capacity reaching up to 50% of host image. Reversible Data Embedding Using a Difference Expansion: Current difference-expansion (DE) embedding functions performs one layer embedding in difference image. Unless current difference image has no expandable differences left the expansion for another layer embedding do not turn to the next difference image. This technique has some disadvantages as image quality may have been severely degraded even before the later layer embedding begins. As the large magnitude of previous layer embedding has used up all expandable differences. We propose a new DE embedding algorithm based on integer Haar wavelet transform, which utilizes the vertical as well as horizontal difference images for data hiding. Here we have introduced a selection mechanism and dynamic expandable difference search. When there is almost no

chance to embed in small differences of the second difference image this mechanism provides even chances to small differences in two difference images by which embedding effectively overcomes the situation where the largest differences in the first difference image are accepted. Reversible Data Hiding: Digital watermarking, often referred to as data hiding, has recently been proposed as a promising technique for information assurance. Owing to data hiding, however, some permanent distortion may occur and hence the original cover medium may not be able to be reversed exactly even after the hidden data have been extracted out. Following the classification of data compression algorithms, this type of data hiding algorithms can be referred to as lossy data hiding. It can be shown that most of the data hiding algorithms reported in the literature are lossy. Here, let us examine three major classes of data hiding algorithm. With the most popularly utilized spreadspectrum water- marking techniques, either in DCT domain [1] or block 8x8 DCT domain [2], round- off error and/or truncation error may take place during data embedding. As a result, there is no way to reverse the stago-media back to the original without distortion. Lossless Generalized-LSB Data Embedding: We present a lossless data-embedding technique, where the exact recovery of the original host image signals upon extraction of the embedded information. As the data-embedding method a generalization of the well-known least significant bit (LSB) modification is proposed. Here Capacity-distortion curve introduces additional operating points. Signals that are used for embedding distortion can transmit compressed descriptions as part of the embedded payload and lossless recovery of the original is achieved by compressing portions. Unaltered portions of the host signal are utilized by prediction-based conditional entropy coder. Here Sideinformation improves the compression efficiency as well as the lossless data-embedding capacity. Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding: Prediction Error Expansion (PEE) reversible data hiding schemes consist of two steps. In First, pixel prediction strategies are utilized by a sharp prediction-error (PE) histogram. In Second, secret messages are reversibly embedded into the prediction-errors through expanding and thus shifting the PE histogram. PEE methods treat the two steps independently and they aim at histogram modification to advance the embedding performance for a PE histogram or either focuses on pixel prediction to obtain a sharp PE histogram. Proposed a new pixel prediction method based on the minimum rate criterion which is used for reversible data hiding. This establishes the consistency between the two steps and optimal embedding performance on the generated PE sequence is optimized by histograms modification scheme. Both final embedding performance and prediction accuracy is demonstrated using previous state-of-art counterparts significantly.

II EXISTING SYSTEM

1) Data encryption using steganography Steganography was getting used in earlier days to send the data to the receiver. The symmetric key is used by both sender and receiver to encrypt and decrypt the data. Disadvantage: As same key is used by both sender and receiver there was highly chances to decrypt the data by the unauthorized person. 2) Data security on the basis of cryptography Cryptography is the way to provide security to prevent the conversation between sender and receiver. It has two types as 1) Symmetric key cryptography

2) Asymmetric key cryptography Symmetric key Cryptography also called as Public key cryptography is better but some disadvantage in that system they are as follows

PROPOSED SYSTEM

The system based on the public key cryptography has advantages over the existing system as it uses two separate keys for the encryption and decryption purpose. Both sender and receiver use the different keys where sender uses the public key and receiver uses the private key. As the sender has public key which is publically visible if third person want to know about the data , person will failed to find the data as it will get opened by the private key of the receiver.

III. GOALS AND OBJECTIVES

To propose a reversible, a lossless and a combined data hiding schemes with probabilistic and homomorphic properties for ciphertext images encrypted by public key cryptosystems.

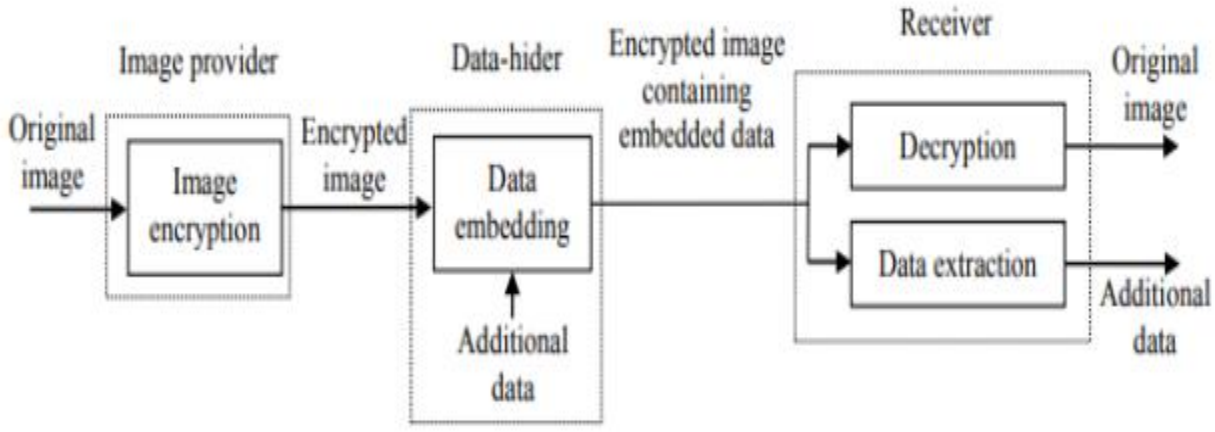

Figure 3.1. Sketch of lossless data hiding scheme for public-key-encrypted images

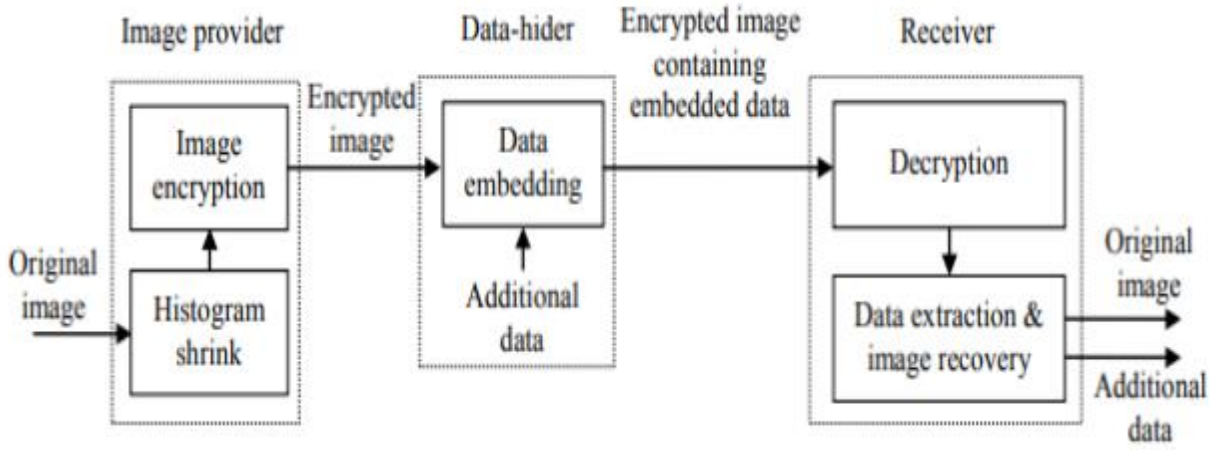

Figure 3.2. Sketch of reversible data hiding scheme for public-key-encrypted images

IV. SCOPE

Future scope A lossless, a reversible, and a combined information hiding plans for figure content pictures scrambled by open key cryptography with homomorphic and probabilistic properties. In the lossless plan, the ciphertext pixel qualities are supplanted with new values for installing the extra information into the LSB-planes of ciphertext pixels. Thusly, the installed information can be straightforwardly removed from the scrambled area, and the information implanting operation does not influence the unscrambling of unique plaintext picture. In the reversible plan, a pre-processing of histogram therapist is made before encryption, and a half of ciphertext pixel qualities are altered for information inserting. On beneficiary side, the extra information can be separated from the plaintext space, and, in spite of the fact that a slight twisting is presented in unscrambled picture the first plaintext picture can be recuperated with no mistake. Because of the two's similarity plots, the information implanting operations of the lossless and the reversible plans can be all the while performed in a scrambled picture. In this way, the collector may remove a piece of installed information in the scrambled space, and concentrate another piece of inserted information and recoup the first plaintext picture in the plaintext area.

4.1 Detailed System Design of NLP

Encryption and information hiding are two viable method for information security. While the encryption procedures change over plaintext content into mixed up ciphertext, the information concealing strategies insert extra information into spread media by presenting slight alterations. In some mutilation unsuitable situations, information concealing may be performed with a reversible or lossless way. In spite of the fact that the expressions "lossless" and "reversible" have a same which means in an arrangement of past references, we would recognize them in this work. We say that information hiding technique is lossless if the display of cover signal containing installed information is same as that of unique cover despite the fact that the spread information have been adjusted for information inserting. For instance, the pixels with the most utilized shading as a part of a palette picture are doled out to some unused shading lists for conveying the extra information, and these files are diverted to the most utilized shading. Thusly, despite the fact that the files of these pixels are modified, the genuine shades of the pixels are kept unaltered. Then again, we say an information concealing system is reversible if the first cover substance can be consummately recouped from the spread rendition containing installed information despite the fact that a slight bending has been presented in information implanting strategy. Various instruments, for example, distinction extension, histogram shift and lossless pressure, have been utilized to build up the reversible information concealing systems for computerized pictures. As of late, a few decent forecast methodologies and ideal move likelihood under payload-mutilation measure have been acquainted with enhance the execution of reversible information covering up. 4.2 Method project progress and algorithm

MODULES:

- Lossless Data Hiding Scheme
- Reversible Data Hiding Scheme
- Combined Data Hiding Scheme

MODULES DESCRIPTON:-

Lossless Data Hiding Scheme

- A lossless data hiding scheme for public-key-encrypted images is proposed. There are three parties in the scheme: an image provider, a data-hider, and a receiver.
- With a cryptosystem possessing probabilistic property, the image provider encrypts each pixel of the original plaintext image using the public key of the receiver, and a data-hider who does not know the original image can modify the ciphertext pixel-values to embed some additional data into the encrypted image by multi-layer wet paper coding under a condition that the decrypted values of new and original cipher-text pixel values must be same.
- When having the encrypted image containing the additional data, a receiver knowing the data hiding key may extract the embedded data, while a receiver with the private key of the cryptosystem may perform decryption to retrieve the original plaintext image.
- The embedded data can be extracted in the encrypted domain, and cannot be extracted after decryption since the decrypted image would be same as the original plaintext image due to the probabilistic property

Reversible Data Hiding Scheme

- This section proposes a reversible data hiding scheme for public-key-encrypted images. In the reversible scheme, a preprocessing is employed to shrink the image histogram, and then each pixel is encrypted with additive homomorphic cryptosystem by the image provider.
- When having the encrypted image, the data-hider modifies the ciphertext pixel values to embed a bitsequence generated from the additional data and errorcorrection codes.

• Due to the homomorphic property, the modification in encrypted domain will result in slight increase/decrease on plaintext pixel values, implying that a decryption can be implemented to obtain an image similar to the original plaintext image on receiver side. Because of the histogram shrink before encryption, the data embedding operation does not cause any overflow/underflow in the directly decrypted image. Then, the original plaintext image can be recovered and the embedded additional data can be extracted from the directly decrypted image.

Combined Data Hiding Scheme

• A lossless and a reversible data hiding schemes for public-key-encrypted images are proposed. In both of the two schemes, the data embedding operations are performed in encrypted domain.

• On the other hand, the data extraction procedures of the two schemes are very different. With the lossless scheme, data embedding does not affect the plaintext content and data extraction is also performed in encrypted domain.

EXPERIMENTAL RESULTS

Four gray images sized 512×512, Lena, Man, Plane and Crowd, shown in Figure 4, and 50 natural gray images sized 1920×2560, which contain landscape and people, were used as the original plaintext covers in the experiment. With the lossless scheme, all pixels in the cover images were firstly encrypted using Paillier cryptosystem, and then the additional data were embedded into the LSB-planes of ciphertext pixel-values using multi-layer wet paper coding as in Subsection 2.B. Table 1 lists the average value of embedding rates when K LSB-planes were used for carrying the additional data in the 54 encrypted images. In fact, the average embedding rate is very close to (1_1/2K). On receiver side, the embedded data can be extracted from the encrypted domain. Also, the original plaintext images can be retrieved by direct decryption. In other word, when the decryption was performed on the encrypted images containing additional data, the original plaintext images were obtained.

With the reversible scheme, all pixels were encrypted after histogram shrink as in Subsection 3.A. Then, a half of ciphertext pixels were modified to carry the additional data as in Subsection 3.B, and after decryption, we implemented the data extraction and image recovery in the plaintext domain. Here, the low-density parity-check (LDPC) coding was used to expand the additional data as a bit-sequence in data embedding phase, and to retrieve the coded bit-sequence and the embedded additional data on receiver side. Although the error-correction mechanism was employed, an excessive payload may cause the failure of data extraction and image recovery. With a larger value of δ, a higher embedding capacity could be ensured, while a higher distortion would be introduced into the directly decrypted image. For instance, when using Lena as the cover and δ = 4, a total of 4.6×104 bits were embedded and the value of PSNR in directly decrypted image was 40.3 dB. When using δ = 7, a total of 7.7×104 bits were embedded and the value of PSNR in directly decrypted image was 36.3 dB. In both of the two cases, the embedded additional data and the original plaintext image were extracted and recovered without any error. Figure 5 gives the two directly decrypted images. Figure 6 shows the rate-distortion curves generated from different cover images and various values of δ under the condition of successful data-extraction/image-recovery. The abscissa represents the pure embedding rate, and the ordinate is the PSNR value in directly decrypted image. The rate-distortion curves on four test images, Lena, Man, Plane and Crowd, are given in Figures 6, respectively. We also used 50 natural gray images sized 1920×2560 as the original plaintext covers, and calculated the average values of embedding rates and PSNR values, which are also shown as a curve marked by asterisks in the figure. Furthermore, Figure 7 compares the average rate-PSNR performance between the proposed reversible scheme with public-key cryptosystems and several previous methods with symmetric cryptosystems under a condition that the original plaintext image can be recovered without any error using the data-hiding and encryption keys. In [11] and [12], each block of encrypted image with given size is used to carry one additional bit. So, the embedding rates of the two works are fixed and low. With various parameters, we obtain the performance curves of the method in [15] and the proposed reversible scheme, which are shown in the figure. It can be seen that the proposed reversible scheme significantly outperforms the previous methods when the embedding rate is larger than 0.01 bpp.

With the combined scheme, we implemented the histogram shrink operation with a value of parameter δ, and encrypted the With the combined scheme, we implemented the histogram shrink operation with a value of parameter δ, and encrypted the pixels using Paillier cryptosystem. Then, we embedded the first part of additional data into the ciphertext pixel values by the reversible embedding method, and embedded the second part of additional data into the K LSB-planes of the ciphertext pixel values by the lossless embedding method. When having the encrypted image containing the additional data, we firstly extracted the second part of additional data from the LSB-planes of ciphertext pixel values. After decryption, we further extracted the first part of additional data and recovered the original plaintext image in the plaintext domain. Here, the payloads of the two parts of additional data are same as the payloads of reversible and lossless schemes, respectively, and the quality of directly decrypted image is same as that of reversible scheme.

(a) (b) (c) (d)

Figure 4. Cover images (a) Lena, (b) Man, (c) Plane and (d) Crowd

Table 1. Average payload of lossless scheme with respect to different *K*

K	1	2	3	4	5
Average embedding rate (bits per pixel) with Paillier cryptosystem	0.499	0.749	0.875	0.937	0.968

Figure 6.1 Cover images (a) Lena, (b) Man, (c) Plane and (d) Crowd.

Figure 6.2. Directly decrypted Lena of reversible scheme (a) δ = 4, a total of 4.6×104 bits embedded and PSNR = 40.3 dB, (b) δ = 7, a total of 7.7×104 bits embedded and PSNR = 36.3dB

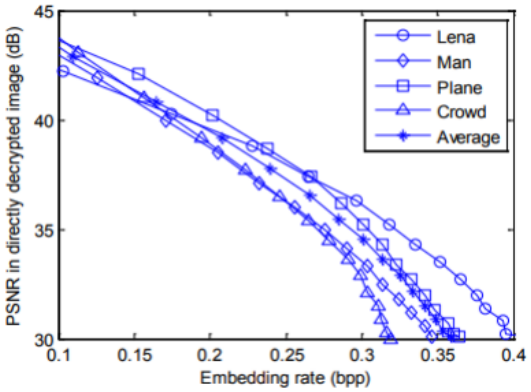

Figure 6.3 Embedding rate-distortion performance of reversible scheme on different cover images

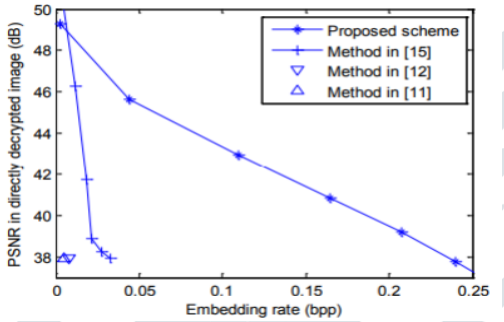

Figure 6.4 Comparison of rate-PSNR performance between the proposed reversible scheme and previous methods

VI. CONCLUSION

This work proposes a lossless, a reversible, and a combined data hiding schemes for cipher-text images encrypted by public key cryptography with probabilistic and homomorphic properties. In the lossless scheme, the ciphertext pixel values are replaced with new values for embedding the additional data into the LSB-planes of ciphertext pixels. This way, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. In the reversible scheme, a preprocessing of histogram shrink is made before encryption, and a half of ciphertext pixel values are modified for data embedding. On receiver side, the additional data can be extracted from the plaintext domain, and, although a slight distortion is introduced in decrypted image, the original plaintext image can be recovered without any error. Due to the compatibility of the two schemes, the data embedding operations of the lossless and the reversible schemes can be simultaneously performed in an encrypted image. So, the receiver may extract a part of embedded data in the encrypted domain, and extract another part of embedded data and recover the original plaintext image in the plaintext domain.

VII. FUTURE SCOPE

An efficient method of completely separable reversible data hiding in encrypted images is proposed. The cover image is first partitioned into non-overlapping blocks and specific encryption is applied to obtain the encrypted image. Then, image difference in the encrypted domain can be calculated based on the homomorphic property of the cryptosystem. The data hider, who does not know the original image content, may reversibly embed secret data into image difference based on two-dimensional difference histogram modification. Data extraction is completely separable from image decryption; that is, data extraction can be done either in the encrypted domain or in the decrypted domain, so that it can be applied to different application scenarios. In addition, data extraction and image recovery are free of any error.

VIII.REFERENCES

[1] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253_266, Feb. 2005.

[2] M. U. Celik, G. Sharma, and A. M. Tekalp, "Lossless watermarking for image authentication: A new framework and an implementation," IEEE Trans. Image Process., vol. 15, no. 4, pp. 1042_1049,Apr. 2006.
[3] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354_362, Mar. 2006.
[4] X. Li, W. Zhang, X. Gui, and B. Yang, "A novel reversible data hiding scheme based on two- dimensional difference-histogram modification," IEEE Trans. Inf. Forensics Security, vol. 8, no.7, pp. 1091_1100, Jul. 2013.
[5] C. Qin, C.-C.Chang, Y.-H.Huang, and L.-T. Liao, "An inpaintingassisted reversible steganographic scheme using a histogram shifting mechanism," IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 7, pp. 1109_1118, Jul. 2013.
[6] W.-L. Tai, C.-M.Yeh, and C.-C. Chang, "Reversible data hiding based on histogram modification of pixel differences," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 6, pp.906_910, Jun. 2009.
[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] Y. Hu, H.-K. Lee, and J. Li, "DE-based reversible data hiding with improved overflow location map," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 2, pp. 250_260, Feb.2009.
[9] X. Li, B. Yang, and T. 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.