Lossless and Reversible Data Hiding using Public Key Cryptography

POOJA SHETYE{e-mail: pooja.shetye118@gmail.com}, *SRUSHTI* VAREKAR, *MANALI* ZAJAM, and *MONIKA* PAWAR *SUJATA* KADAM{e-mail: sujatakadam7890@gmail.com}

[1]R.A.I.T, DEPARTMENT OF EXTC ENGG.

Abstract. - In today's world, the internet is a platform, where large amount of data can be obtained and transferred. Different technologies and internet access are used to transfer the data which can be accessed by authorized and unauthorized users.The major drawback of these technologies are that any unauthorized person can access it.Hence encryption and decryption is perform on Message/Data .In encryption the plain text/image is converted into cipher text/image.The technique of data hiding is used to hide the data that has to be transferred from the source to the destination.The process involves insertion of secret message in the cover image which is encrypted with the help of AES algorithm. This algorithm generates public/private key. All this process can be performed in lossless and reversible manner.

Keywords- Data hiding,lossless,reversible,algorithm

1 Introduction

Day by day with the rapid advancement of information technology enormous images and data are available on the internet.It alarms for a need to provide some kind of certification on such significant data. when we transfer any image,data to the receiver there might be possibility that any intruder is present and may obtain the confidential data .After apprehending the image, the trespasser may view the meaningful subject in the image. This may not matter in some cases. But in medical and military field images with distortion is unacceptable. This process involves embedding of some secret information in carrier signal. For copyright protection and covert communication the properties of less importance are changed. Generally,the data hiding process will result in degradation of properties in host signal. Application like law enforcement, system of medical images expects to reverse the the modified image back to original image for legal reasons ,whereas in application like remote sensing and military imaging high precision is expected. In some scientific research, practical data are expected to be obtained. In these situations, the reversibility of the image is expected. This technology is used in many application like in certification, military, medical and law enforcement.

CRYPTOGRAPHY

Cryptography is a worldwide well-known process in which plain text is encrypted to generate cipher (encrypted) text. Plain text is data that can be read and understood easily without any special measures. When plain text is encrypted unreadable text is generated called as cipher text. In short cryptography converts data to make sure of secrecy as genuine nature of information and data is transmitted through insecure networks .it facilitates the secure transfer to authorized recipient. Cryptography consists of two branches cryptolog and cryptanalysis. Cryptology aims at keeping plain text secret from impertinent person, while cryptanalysis creates such techniques to recover original information which is considered authentic. Basically, all cryptographic processes have four basic parts.

• Plain text - Untangled information for example sensitive information like a credit card number, password, a bank account number, pay-roll data, personnel information, or a secret formula is transmitted between organizations.

• Cipher text- Mathematical algorithm renders plain text into unintelligible Cipher text.This encrypted plain text is transported to receiver.

• Key- A mathematical value, formula, or process decides how a plain text message is encrypted or decrypted . The key is the only way to work out the secret information.

• Cryptographic Algorithm – This is a mathematical method which is used to convert the data from plain text form to cipher text form.By using the cryptographic algorithm we convert plain text form to cipher text form which is referred as encryption and the process of converting cipher text form back to plain text form by using the same technique reversibly is called as decryption.To make secure communication there's illustration of steps below for secret key cryptography

The technique of cryptographic system which uses both the keys namely public key and private key is known as technique of public-key cryptography or asymmetric cryptography. Such keys are generated by mathematical problem based cryptographic algorithm. For efficient security only private key is expected to kept private whereas public key can be disclosed without hesitation.Due to which the receiver is able to receive the message but while decryption is not possible to access because the private key is kept secret. Sometimes combining a message with private key i.e a short digital signature on message is generated. To verify validity of signature the corresponding public key is combined message with digital signature and authenticated using known public key. This is process involved in robust authentication The applications and protocols of public key algorithm assuring the secretiveness, certification and non-contradiction of electronics communications and data storage makes it prime element in modern cryptosystems.Various internet standards underpinned by public key algorithm are Transport Layer Security (TLS), S/MIME, PGP, and GPG. All in all public key provides, key distribution and confidentiality and digital signature.

1.2 Fundamentals of Reversible Data Hiding (RDH):

Following are the approaches used in RDH:
1] After encryption little space is vacated to hide the data.
2] First room is vacated in original media and then the encrpytion technique is processed for image encryption.

As in the first approach due to encryption modification of image takes place makes it difficult to vacate room for hiding data whereas in second approach no difficulty is faced and procedure is carried on efficiently.

1.3 To measure the performance of the RDH techniques following parameters :

To measure the performance of RDH technique following are the steps taken :
There are various methods of hiding data reversibly in an image. Any one among them expected to benefit us. The parameters are as follows:
• Quantity of Data: It facilitates hiding of maximum amount of data in the image.
• Complexity of technique: usability of technique depend on simpler and complex nature of technique.
• Quality of cover image: it suggest the quality of image is significant because if the quality of original image is spoiled after extracting message it will not tolerated in RDH.

2 LITERATURE SURVEY

Lichin Huang[8] proposed the histogram shift method for reversible data hiding from all the various data embedding techniques.

The histogram shift method is done by shifting the histogram in a fix direction, where there are two important points which are peak and zero point. The peak point resembles to grey scale value's maximum pixel number in image and the zero-point, minimum pixel value that is zero in the given histogram image. At the embedding process, in this histogram shift-based algorithm, the pixel in peak and zero point are modified in such a way that the pixel in the peak point carries a bit of secret message while the other doesn't carry any secret data.

For increasing the embedding capacity, Yeh[4] proposed a predict error method for data embedding. In this method, the cover image is divided in two block and a center point is obtained and prediction error value is obtained between it and its surrounding pixel values. The predict error value histogram is drawn and is peak value is found while the secret data in embedded a two side of peak point.

Intended on further better hiding capacity, J. Tian[5] has presented a Difference Expansion (DE) technique which gives an added storage space for dismissal of any useless content in image. In this, difference between the adjacent pixel is collected and some values are selected for further DE process. This method is best for visual quality and capacity limit.

In this paper we have anticipated lossless and reversible data hiding technique using public key cryptography which is further explained.

3 DATA HIDING USING ENCRYPTION

Reversible data hiding and visual crptography methods are included in the encryption process where the text is hide in reversible manner. The Tian's paper has proposed the scheme of difference expansion which is only applicable for gray scale images where,it gives an extra storage space by exploring the dismissal in the image media.In our approach we have personalized this method for colour images by reversibly data hiding in each colour component individually, which also increases the space to hide data. Basic technique for obtaining the reversed data is by selecting an area from an image, where this image is first converted into binary format to form a pixel matrix. Then the binary value of LSB that is the unit place value of selected matrix are interchanged with the binary value of data. Similarly all binary bits of the data to be hidden are embedded on image through same bit value change technique. By using this technique the data is divided and separately inserted at each pixel of matrix. This will help to sustain the quality and intensity of the cover image in which secret message or data is hidden. The PSNR value can be used to differentiate the feature of cover and original image. For protection of cover image instead of using pattern cipher,we used public or private key (i.e. the password of certain length is entered for obtaining the data). This method is plain and the output obtained will be initial image with the hidden data. The PSNR of the output image is kept to infinity which imports that the image is same as the initial image.

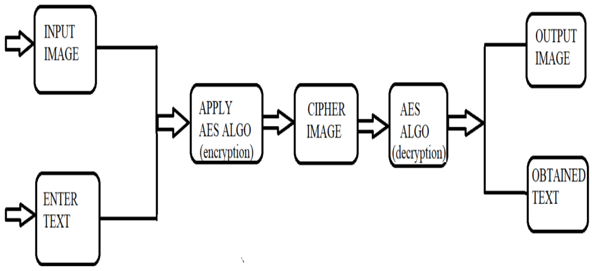


Figure 1. DATA HIDING PROCESS

4 ALGORITHM:

AES ALGORITHM

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm. The AES has three exact 128-bit block ciphers with secret key sizes are 128, 192 and 256 bits. Key extent is infinite, whereas the maximum block size is 256 bits.Substitution-permutation network (SPN) is used while plaining AES whereas the Data Encryption Standard (DES) Feistel network is not used.

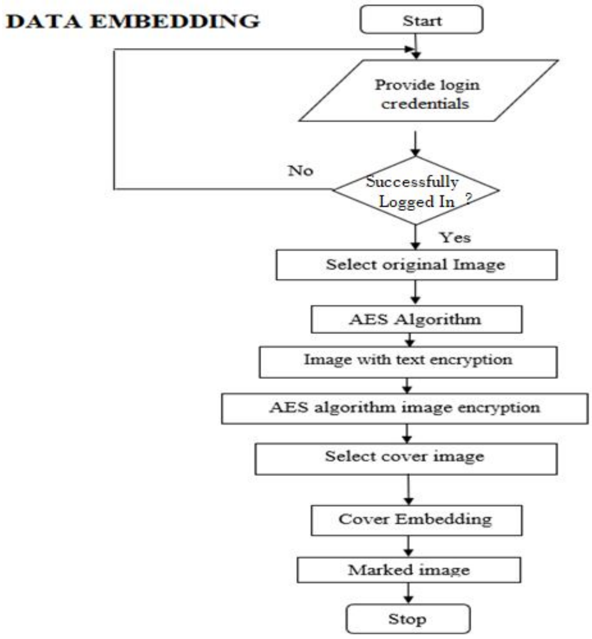


Figure 2. ENCRYPTION FLOWCHART

• Key Expansions:AES consists of a distinct 128-bitround key chunk for every another chunk.This technique of key expansion algorithm takes an input of a four-word key and the product obtained is a lined array of 44 words i.e.176 bytes.

• Opening Step

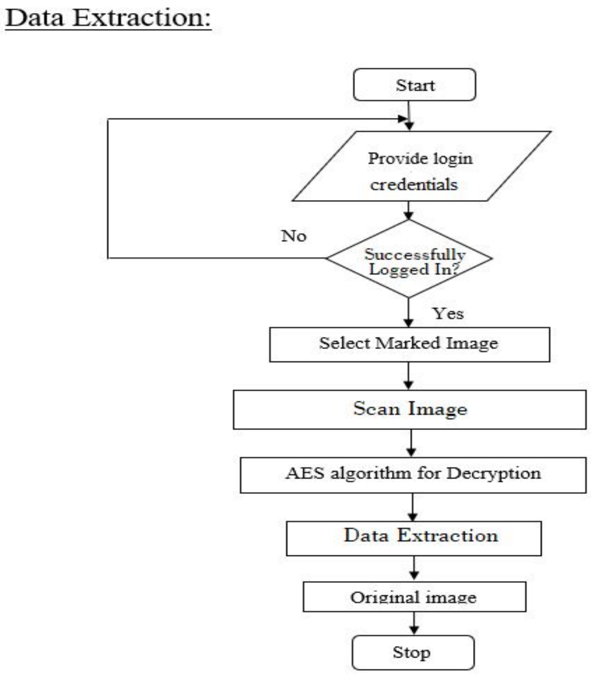


Figure 3. DECRYPTION FLOWCHART

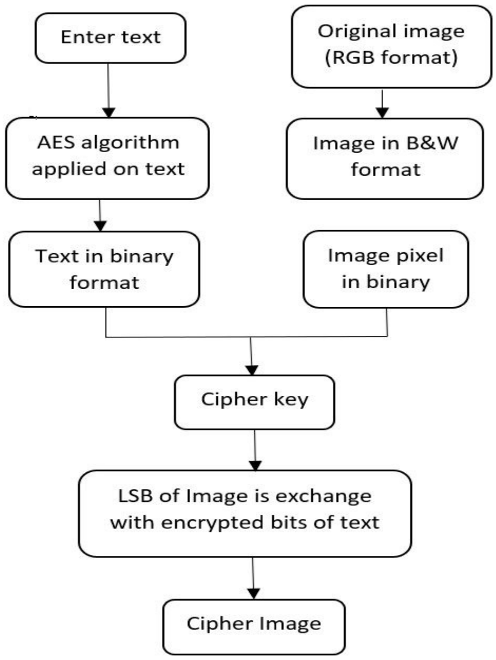

Enter text
Original image (RGB format)
AES algorithm applied on text
Image in B&W format
Text in binary format
Image pixel in binary
Cipher key
LSB of Image is exchange with encrypted bits of text
Cipher Image

Figure 4. ENCRYPTION PROCESS

o Add Round Key:Every byte is united with a block of a round key, this is done by using bitwise xor.

• What are Rounds?

o Sub Bytes—Each byte is interchanged with another byte according to a lookup table.

o Shift Rows—The last three rows of the state are shifted cyclically to a firm number of steps.

o Mix Columns—In this step a mixture of columns occurs and the output is a four byte in every column.

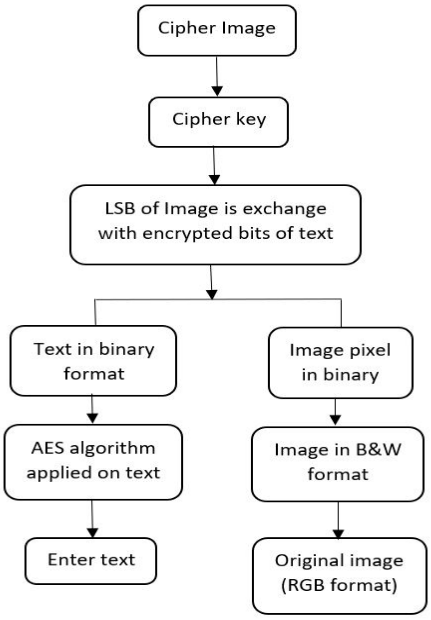

Cipher Image
Cipher key
LSB of Image is exchange with encrypted bits of text
Text in binary format
Image pixel in binary
AES algorithm applied on text
Image in B&W format
Enter text
Original image (RGB format)

Figure 5. DECRYPTION PROCESS

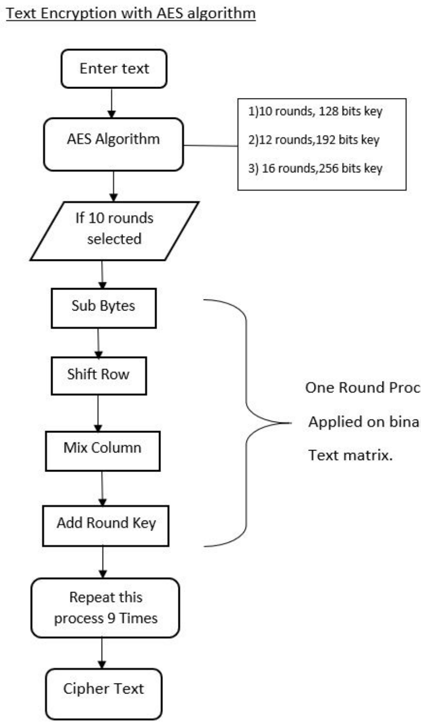


Figure 6. TEXT ENCRYPTION

o Further add the RoundKey

- Last Step (no compound Columns)

This is also similar to upper one just the one step is not required in it. The steps involved in it are sub byte, shift row and add round key.

Encryption with AES:

AES (Advanced Encryption Standard)

Nowadays largely adopted uniform encryption algorithm fitting to be encountered (AES). Its six time faster than tripple DES

As key size was much smaller it led to replacement of DES. Due to greater computing power , it is specified as sensitve towards intensive attack of key search. to overcome this shortcoming led to invention of tripple DES which was discovered to be slow.

Following are features of AES –

1] Software implementable in C and Java

2] 128-bit data, 128/192/256-bit keys

3] Provide full specification and design details

4] Symmetric key block cipher

5] Stronger and faster than Triple-DES

5 RESULT

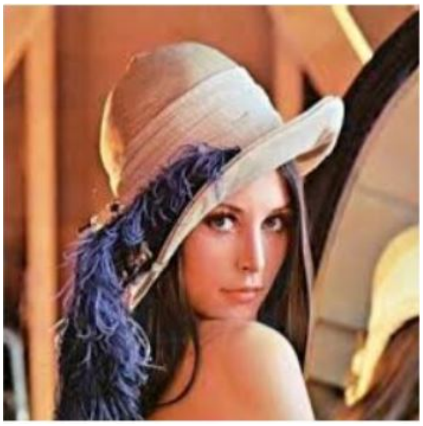


Figure 7. Original image of Lena - size 28.7 KB

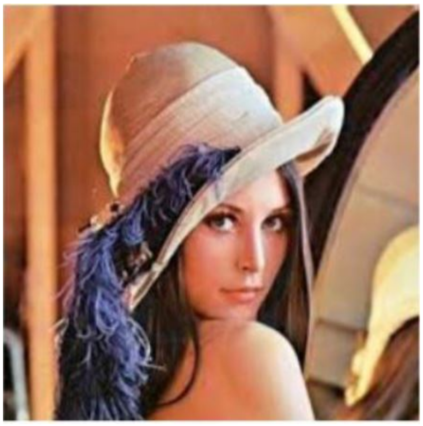
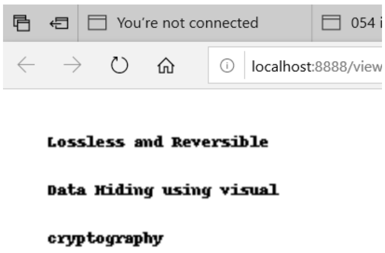


Figure 8. Encrypted image of Lena - size 174 KB



Lossless and Reversible

Data Hiding using visual

cryptography

Figure 9. Decoded message after decryption process

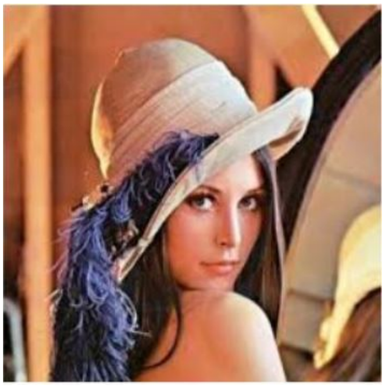


Figure 10. Decoded image of Lena after decryption process - size 27.9 KB

The first image taken, which is the original image (fig 4)of size 28.7KB with pixel resolution of 550X824. The input text which has to be hidden is encrypted in image. The encrypted image obtain by interchanging 8 bit pixel value with the binary value of data which is called as cipher image(fig 5). Here the size of image gets increase and can go to 174KB but the pixel resolution remains unchanged. The data is hided in the image by using encryption algorithm and thus forms a cipher image. The last image shows decoded image (fig 6) where the data is remove from the cipher image,whose size is similar to the original size. Histogram graph and PSNR value are used to compare the quality and noise between original image and encoded image.Here the histogram of original and encoded image has some minute differences such as the colour of graph but overall both histogram are similar.

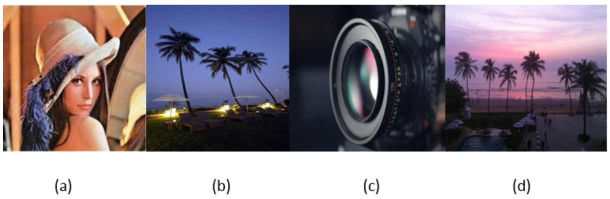


Figure 11. (a)LENA (b)BEACH (c)CAMERA (d)SUNSET

Table 1. Comparison of images with different parameters

Image name	PSNR value	Original size (KB)	Encrypted size (KB)	Decrypted size (KB)
LENA	8.308	28.7	174	27.9
BEACH	6.057	74	219.3	73.5
CAMERA	4.760	51	196.3	50.3
SUNSET	7.160	44.7	190	44.1

6 HISTOGRAM

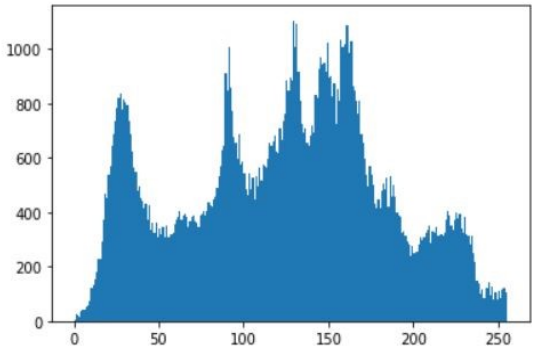


Figure 12. Histogram of original image of LENA

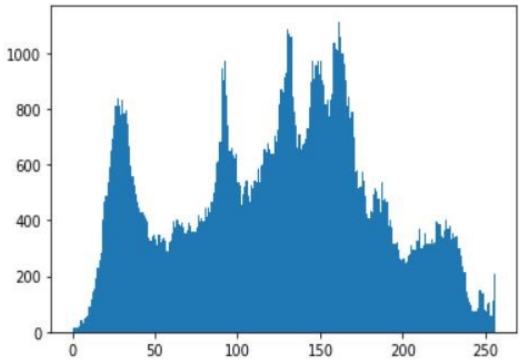


Figure 13. Histogram of encoded image of LENA

7 ADVANTAGES

1.A prediction method which is smarter, is fully used to make the estimated errors almost zero, the performance achieved will be much better, but because of prediction the computation complexity will be higher.

2. The twist or deformation performance of the proposed scheme is superb.

3.A number of subsets are formed by dividing the "input image" and then in the estimated errors of the next subset, the reserved information of a subset is always implanted.

4. This method implant secret data successfully and get the original data in the subsets inversely.

5. Using this technique one can solve the issue of key distribution in the algorithms of symmetric key.

6. The technique of public key cryptography is not used to replace the technique of secret key cryptography, but rather it is used as a complementary technique, to make the data more secured.

7. The security level of data is increased by using the two keys.

8. Refused digital signatures are provided by this technique.

8 DISADVANTAGES

1) Hiding capacity is low.

2) Data compression is not enough.

3) The image quality of the decrypted images decreases.

4) Speed is one of the disadvantage of public key cryptography technique for encryption; there are many famous encryption techniques based on the secret key cryptography which are much faster and better than the ones, currently used as the encryption techniques for the public key.

5) For imitation the technique of public key cryptography may be not efficient, even if the private key of user is not available.

9 APPLICATIONS

1) This technique provides secrecy to the data, especially for confidential data or secret data in defence forces during communication as most essential thing in this field is to keep the secrecy level of embedded data as high as possible.

2)The cryptography technique provide us the following benefits:

a. Potential to hide the existence of secret data.

b. Due to encryption technique, the difficulty level of detecting the hidden data is high.

c. To enhance the security level of encrypted data.

3) Protects the altered data:

a. In this application area we take the advantage of embedded data's fragility.

b. The data embedded should be more fragile.

4)Biological data safekeeping:

In this, either your eye or finger is scanned and their specific features are saved. Further when you scan your finger it matches the pattern of previously saved image and scanned image. In this,the image of fingerprint is not saved, instead series of binary codes are saved for the verification.

5)Bank customer Credentials:

While visiting a bank website, this website displays cipher text and images. When logged in, bank sends a message to the customer i.e. the OTP. Again, the transaction key i.e.captcha: random alphanumeric, entered for logging in.

10 CONCLUSION

The technique of reversible data hiding that we used, is able to encrypt upto 80KB of image where it's resolution is upto "600 x 600 x 8 gray scale image". Various type of images are encrypted using this algorithm which has profitably applied to often used images such as medical, texture, aerial, and all of the CorelDraw database images. Besides, this algorithm is very simple and the time required to complete this process is short and faster which makes this algorithm best within any other reversible data hiding algorithm.

11 REFERENCES

[1]W. Su, Z. Ni, N. Ansari, and , Y.-Q. Shi , "Reversible Data Hiding,"IEEE Trans. on Circuits and Systems for Video Technology, 16(3),pp. 354-362, 2006.

[2]Hang Cheng,Xinpeng Zhang, Zichi Wang, , Jing Long and , "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography", in IEEE Transactions on Circuits and Systems for Video Technology.

[3International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 5, Issue 7,July 2016 Copyright to IJARCCE DOI 10.17148/IJARCCE.2016.5764 321 Lossless and Reversible Data Hiding Mayuri B. Lokhande1,Prof. N. G. Pardeshi.

[4]Yeh, "Reversible data hiding scheme based on prediction error".

[5] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, 2003.

[6] X. Zhang, "Separable Reversible Data Hiding in Encrypted Image," IEEE Trans. Information Forensics Security, 7(2), pp. 526-532,2012.

[7] X. Zhang, "Reversible Data Hiding with Optimal Value Transfer," IEEE Trans. on Multimedia, 15(2), 316-325, 2013.

[8]Lichin Huang has proposed the method for reversibly hiding the data inthe image using histogram shift method.

[9]A. M. Darwish, N. A. Saleh, S. I. Shaheen, H. N. Boghdad , "High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis," Digital SignalProcessing, 20, pp. 1629-1636, 2010.