iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Efficient Image Encryption Technique by Reserving Room Before Encryption

Pradeep Kumar[1], Baswaraj Gadgay[2], Veeresh Pujari[3]
[1]PG Student VLSI Design and Embedded System Department, Visvesvaraya Technological University
[2]PG Coordinator /SO VLSI Design and Embedded System Department, Visvesvaraya Technological University
[3]PG Course Coordinator VLSI Design and Embedded System Department, Visvesvaraya Technological University

Abstract: ***In this paper, a modified version of Zhang's reversible data hiding technique in encrypted image is proposed. In the original method, average value of neighboring pixels is used for block smoothness calculation which fails to give good performance. In proposed work, an enhanced function for measuring smoothness is adopted to reduce the bit error rate. The simulation results show that the performance of proposed method outperforms Zhang's work. For Instance, when block size is 8×8, bit error rate of Lena image in Zhang's method is 1.21% whereas in proposed scheme it reduces to 0.85%. Therefore, by using proposed system more information can be sent without any error.***
Keywords— Data hiding, image encryption, image restoration, reversible data hiding.

I. INTRODUCTION

The internet has become user friendly with the introduction of web browser in 1993 and people can download pictures, movies, videos very easily through the internet. However, the content owner finds a high risk of piracy because of it. Pirates can easily record and distribute copyright protected material without appropriate compensation being paid to the actual copyright owners. Thus, content owners are eagerly seeking technologies that promise to protect their rights. Encryption and data hiding has the potential to fulfil this need. These are two effective means of privacy protection and secret communication.

Data hiding is a process of hiding information into cover media like image, audio, video, text and picture. Reversible data hiding means that information bits are first embedded into the host media by modifying them and then the exact restoration of the original host media is possible after the extraction of hidden information without any distortion. In recent years, several reversible data hiding methods have been introduced. Tian et al. [1] propose a reversible data hiding method based on the difference expansion technique where data hiding is done in the difference of bits. A lossless compression technique is exploited to create extra spaces for carrying additional data in [2]. Ni et al. [3] utilize the minimum and maximum point of the image histogram and embed the data by shifting the histogram. An additive interpolation error expansion technique is adopted in [4] which provide very small falsification and comparatively high capability. Moreover, to improve the performance, different schemes have been proposed into the typical reversible data hiding approaches in [5]-[7].

Usually, data hiding is used for secret communication. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analyzed to expose the existence of the embedment [8]–[10]. In many fields, like legal, medical and military encrypting the image before data hiding and recovering the exact original image after data extraction are two desirable properties. In this case, the host image is encrypted by the content owner before passing it to the data hider for data embedding. The receiver side can extract the hidden information and recover the original host image without any loss or distortion. For example, in [11]-[13] the host image is encrypted before data embedding is actually performed.

In [11], the original host image is first encrypted by using an encryption key. Then the encrypted image is divided into nonoverlapping blocks of same size. After that, by adopting bit flip mechanism one bit of information is embedded in each block. The data extraction and image restoration is performed by examining the smoothness of each block using 1. Nevertheless, in Zhang's system average value of neighbor

$$f = \sum_{u=2}^{s-1}\sum_{v=2}^{s-1} \left| \mathrm{p}(u,v) - \frac{p(\mathrm{u}-1,\mathrm{v}) + \mathrm{p}(\mathrm{u},\mathrm{v}-1) + \mathrm{p}(\mathrm{u}+1,\mathrm{v}) + \mathrm{p}(\mathrm{u},\mathrm{v}+1)}{4} \right| \quad (1)$$

This work proposes a modified reversible data hiding scheme for encrypted image, which is consists of encryption of image, data hiding and data extraction and image restoration. The original host image is completely encrypted by using an encryption key

before sending it to the data hider. Then, the information bits are concealed by modifying a small portion of encrypted data. Finally, at receiver side, the hidden bits are successfully extracted and the original host image is exactly restored without any distortion by means of spatial correlation in natural image. For smoothness calculation, the actual value of neighboring pixel is used instead of average value to reduce the bit error rate. For this reason, the accuracy of the data extraction is further increased.
The rest of this paper is organized as follows. The proposed method is described in Section II. Then, the experimental results are discussed in section III. Finally, Section IV concludes the paper.

II. PROPOSED METHOD

The proposed method is divided into three segments as shown in fig.1. First part is encryption of image, second one is data hiding and the last part is data extraction and image restoration.

A. Encryption of Image

The Symmetric key cryptography is used for the encryption process. The host image is encrypted by an encryption key using a standard stream cipher. It is assumed that, H is an uncompressed host image of size $M \times N$ in which every pixel is represented by 8 bits. $H_{i,j}$ is pixel gray value at position (i, j) and $H_{i,j,k}$ denotes 8 bit binary digits of each pixel where $k=[0,7]$.The relation between bit in a pixel and pixel gray value is denoted by

$$H_{i,j,k} = [\frac{H_{i,j}}{2^k}] \bmod 2, 0 \le k \le 7 \qquad (2)$$

$$H_{i,j} = \sum_{k=0}^{7} H_{i,j,k}.2^k \qquad (3)$$

And

To encrypt the original image a random sequence, $K_{i,j,k}$ is generated according to the encryption key. Then a bitwise exclusive or (XOR) of H and K is performed using the following equation

$$H'_{i,j,k} = H_{i,j,k} \oplus K_{i,j,k} \qquad (4)$$

.

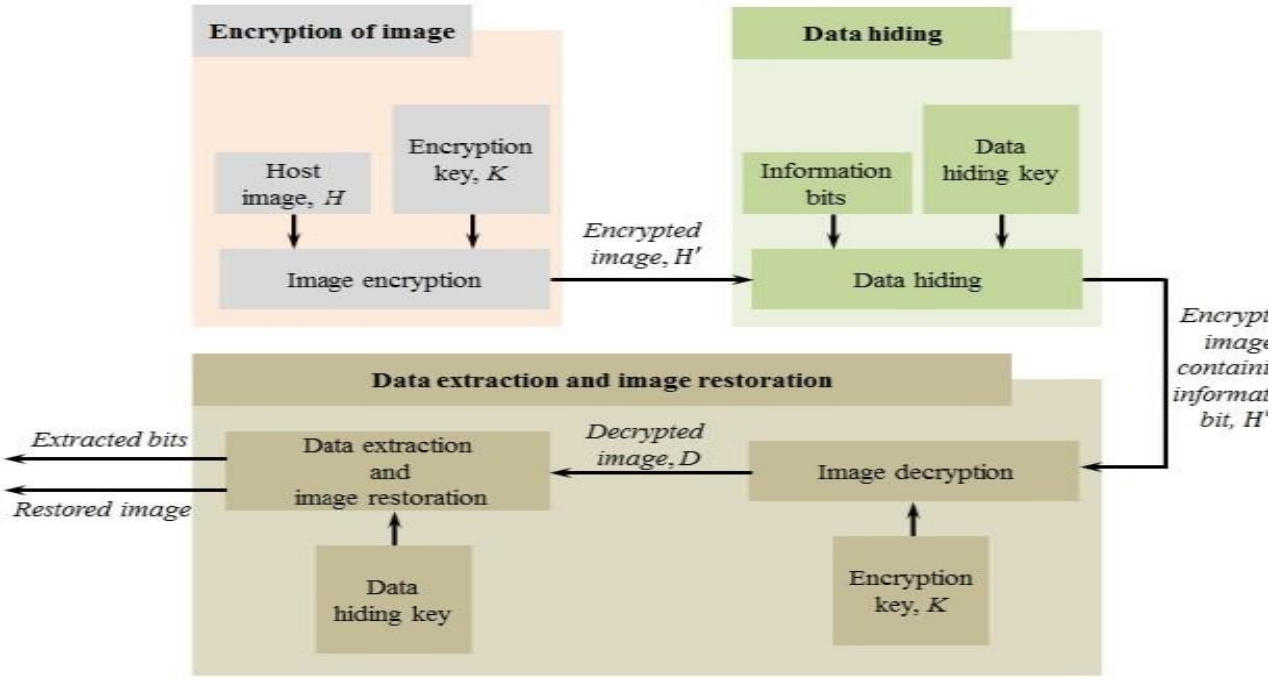


Figure 1. Block diagram of proposed method.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

B. Data Hiding

As the image is encrypted, the data hider will not know anything about the host image but still he can insert data in the encrypted image, *H'* according to following process. Firstly, the encrypted image is divided into a number of no overlapping blocks of size *s*×*s*. Each block will contain one bit of information. Then, according to the data hiding key, the pixels of each block is divided into two sets *A0* and *A1* pseudo randomly. The probability that a pixel belongs to one of two sets is uniformly distributed.If bit to be inserted is '0' then three least significant bits (LSB) of each pixel in set, A0 are flipped i.e.

$$H''_{i,j,k} = \overline{H'_{i,j,k}} \qquad (5)$$

Here, (*i, j*) belongs to set, *A0* and $0 \le k \le 2$. Pixels in set *A1* remain unchanged.

On the other hand, if bit to be inserted is '1' then three least significant bits (LSB) of each pixel in set, *A1* are flipped i.e.

$$H''_{i,j,k} = \overline{H'_{i,j,k}} \qquad (6)$$

Here, (*i, j*) belongs to set *A1* and $0 \le k \le 2$. Pixels in set *A0* are not changed.

The five most significant bits (MSB) of each pixel in both sets remain same only the three LSB are changed. Then the encrypted image containing information bits, *H''* is sent to the receiver.

C. Data Extraction and Image Restoration

After receiving the embedded encrypted image, *H''* a receiver first decrypts the image. By using the encryption key, the image is decrypted by applying bitwise exclusive or (XOR) of received data and random sequence *K*.

$$D_{i,j,k} = H''_{i,j,k} \oplus K_{i,j,k} \qquad (7)$$

The first five most significant bits (MSB) of the decrypted image are identical to the original image.

Then, the decrypted image is partitioned into non overlapping blocks of size *s*×*s*. According to the data hiding key, the pixels of each block are divided into two sets *A0* and *A1* pseudo randomly in the same way as before. For each decrypted block, two new blocks *B0* and *B1* are obtained. In *B0* all the three LSB of each pixel in *A0* are flipped and in *B1* all the three LSB of pixels in *A1* are flipped. Either *B0* or *B1* is the original block and another one is seriously fluctuated block because of three LSB flip.

determine which one is original block, smoothness of *B0* and *B1* are calculated according to the following equations, respectively.

$$f_{B0} = \sum_{u=1}^{s-1}\sum_{v=1}^{s-1} \left| B_0(u,v) - B_0(u+1,v) \right| + \left| B_0(u,v) - B_0(u,v+1) \right| \qquad (8)$$

$$+ \sum_{u=s-1}^{s-1} \left| B_0(u,v) - B_0(u+1,v) \right| + \sum_{v=s-1}^{s-1} \left| B_0(u,v) - B_0(u,v+1) \right|$$

$$f_{B1} = \sum_{u=1}^{s-1}\sum_{v=1}^{s-1} \left| B_1(u,v) - B_1(u+1,v) \right| + \left| B_1(u,v) - B_1(u,v+1) \right| \qquad (9)$$

$$+ \sum_{u=s-1}^{s-1} \left| B_1(u,v) - B_1(u+1,v) \right| + \sum_{v=s-1}^{s-1} \left| B_1(u,v) - B_1(u,v+1) \right|$$

Smoothness of the original block is generally lower than that of the seriously fluctuated one due to the spatial correlation in natural image. Hence, by comparing f_{B0} and f_{B1} data extraction and image restoration can be performed. If $f_{B0} < f_{B1}$, then *B0* will be the original block and '0' will be the extracted hidden bit. Otherwise, *B1* will be the original block and '1' will be the extracted hidden bit. Eventually, extracted hidden bits are concatenated to get the information and restored blocks are collected to make the host image.

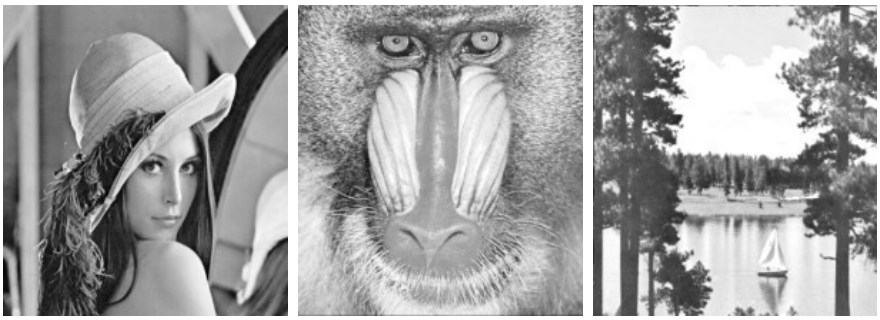
Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

III. EXPERIMENTAL RESULTS

In our simulation, we have used three gray level images such as Lena, Baboon and Sailboat of size 512×512, as host images, as shown in fig.2. These images can be obtained from USC-SIPI image database [14]

As shown in fig. 3(a) host image, Lena was encrypted to generate the encrypted version of it as presented in fig. 3(b). Then, we embedded 1024 bits into the encrypted image by using each block of size 16×16 as given in fig.3(c).After that, the image was decrypted as represented in fig. 3(d). Finally, the hidden information bits were successfully extracted and the original image was perfectly restored from the decrypted image.

Fig.4. represents the bit error rate (%) with respect to block size, s. The error rate is the ratio of unrecovered bits to the total number of bits. According to this fig. bit error rate (%) and block size are inversely proportional. When the block size decreases bit error rate increases and the error rate declines as the block size rises. However, with the increment of block size embedding capacity also decreases as we insert one bit in each block. Moreover, BER performance of Lena is better than that of baboon and sailboat images since spatial correlation of Lena image is stronger than that of others. That means error rate in data hiding system increases because of weak spatial correlation too.



(a) (b) (c)

Figure 2. Host images used for simulation (a) Lena, (b) Baboon, and(c) Sail boat.

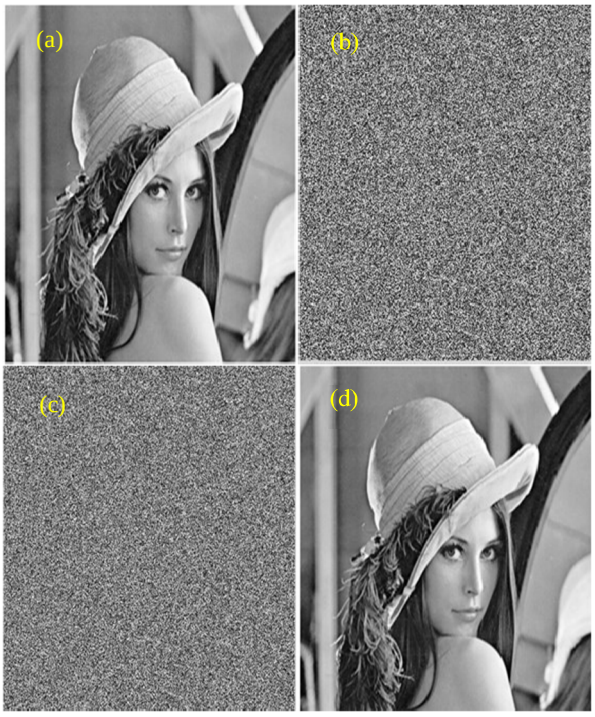


Figure 3. (a) Original Lena, (b) encrypted Lena, (c) encrypted Lena containing information bits, and (d) decrypted Lena containing information bits.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

Fig.5 depicts that proposed method presents lower bit error rates than that of Zhang's system [11] for all three images. For Lena image, as shown in fig. 5(a) when block size is 8×8, the error rate of proposed scheme is 0.85% whereasthe error rate of Zhang's work [11] is 1.21% which is around 1.5 times higher than that of proposed system. According to this fig., by using proposed scheme we can embed at least 1296 (s=14) bits without any error but in case of Zhang's method [11] only 1024 (s=16) bits can be embedded error freely. So, not only in terms of error rate but also in terms of payload proposed method is better than Zhang's one [11]. For the complex image, such as Baboon, the proposed work outperforms the Zhang's work as well. Moreover, for the sailboat image, as shown in fig 5(c), at s=8 the error rate of proposed scheme is 3.3% whereas the error rate of Zhang's method [11] is 6.5 which is approximately 2 times less than that of [11] . Because for smoothness calculation of each block, in proposed method the actual value of neighboring pixels is exploited instead of average value.

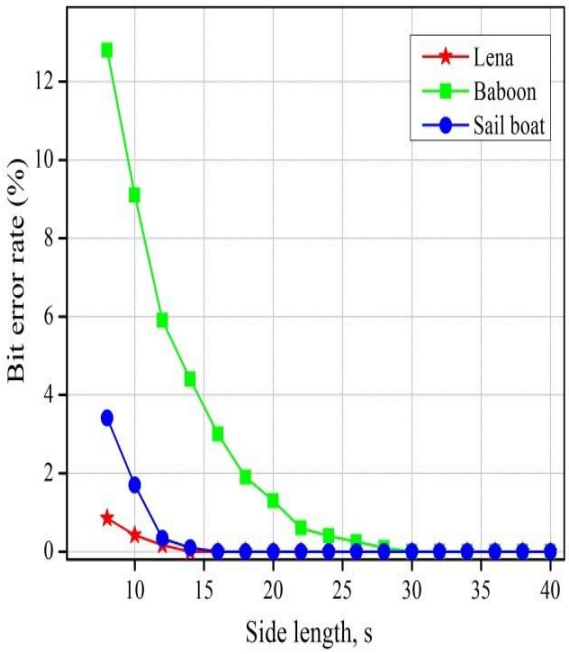
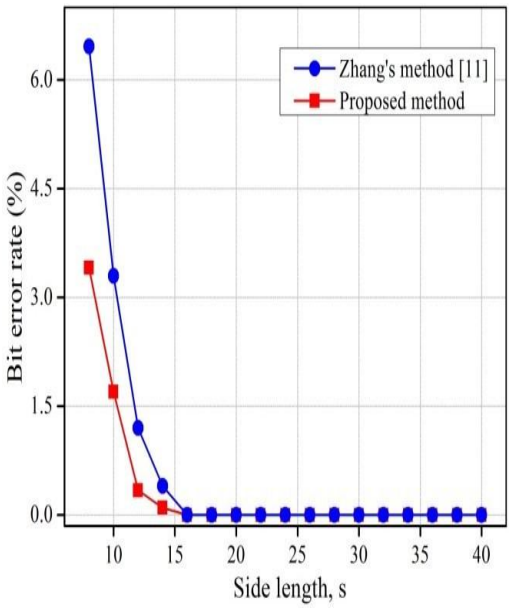
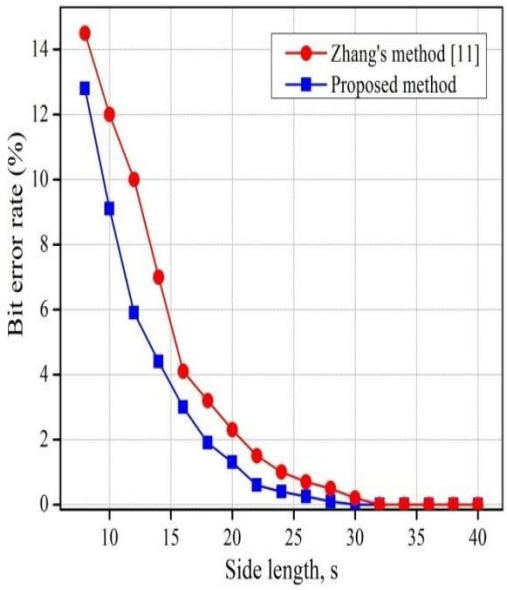


Figure 4. Bit Error rate (%) with respect to block size, *s*.

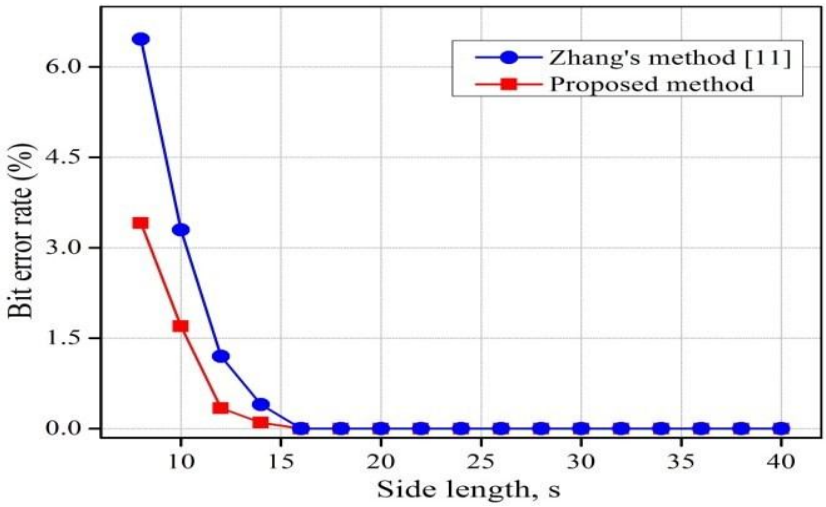


5(a)



5(b)

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



(b)Baboon, and (c) Sail boat..

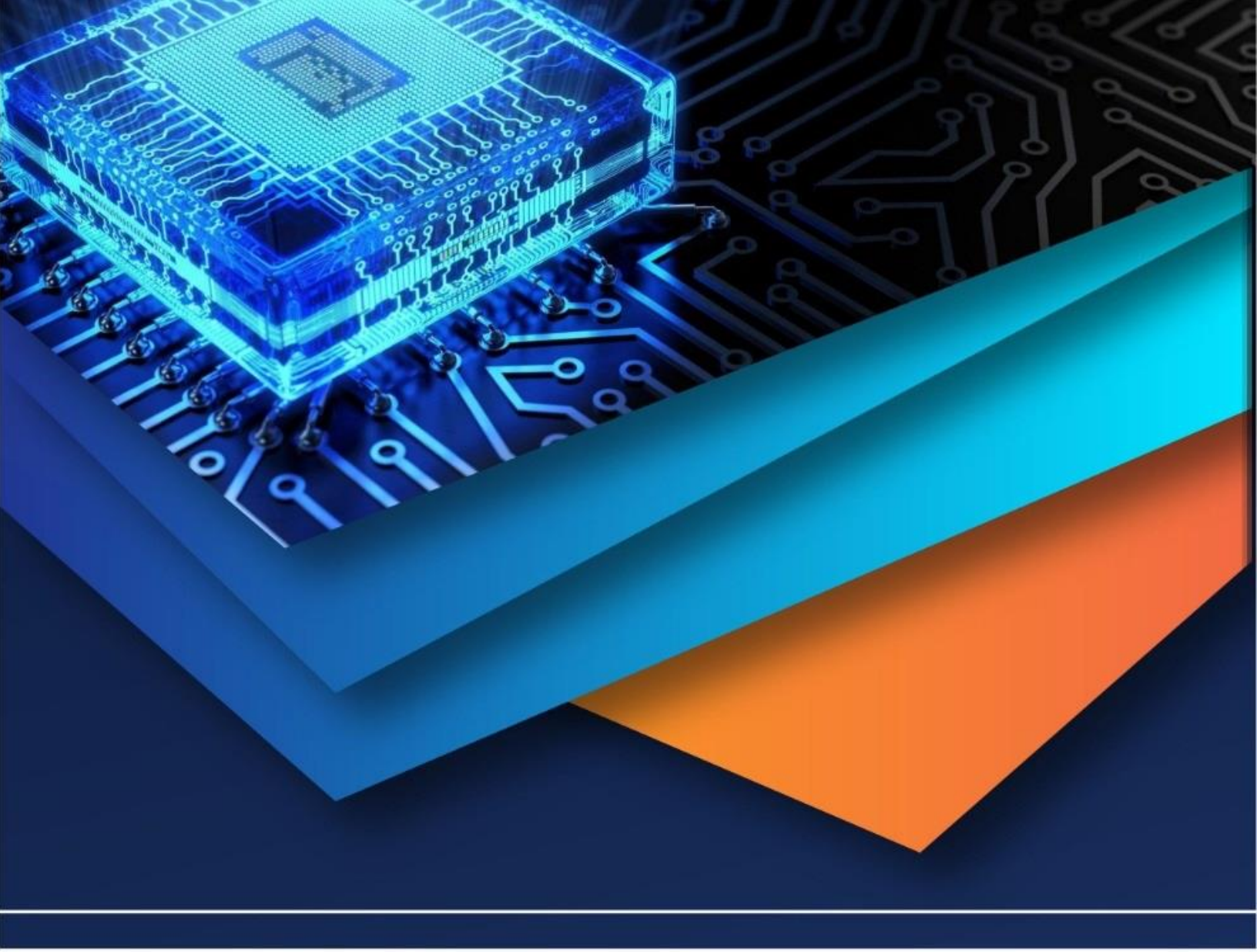
Figure 5. The error rate comparison with Zhang's method for (a) Lena, 5(c)

IV. CONCLUSION

This paper proposes a modified data extraction and image restoration technique based on Zhang's method. A better scheme for calculating smoothness of block is used to reduce the bit error rate of extracted data. To measure smoothness, we have used the real value of adjacent pixels instead of mean value of them. The simulation results demonstrate that the proposed method effectively develops Zhang's work. Moreover, by using proposed system more payloads can be embedded without any error.

REFERENCES

[1] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, 02003.
[2] 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, 2005.
[3] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 8, pp. 354–362, 2006.
[4] L. Luo, Z. Chen, M. Chen, X. Zeng, and H Xiong, "Reversible image watermarking using interpolation technique," IEEE Trans. on Inf. Forensics and Security, vol. 5, no. 1, March, 2010.
[5] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, 2007.
[6] C. C. Chang, C. C. Lin, and Y. H. Chen, "Reversible data-embedding scheme using differences between original and predicted pixel values," Inform. Secur., vol. 2, no. 2, pp. 35–46, 2008.
[7] W. Hong and T. S. Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism," J. Vis. Commun. Image Represent., vol. 22, no. 2, pp. 131–140, 2011.
[8] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," Proc. IEEE, vol. 92, pp. 918–932, 2004.
[9] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, 2007.
[10] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured haar transform domain," Signal Process.: Image Commun., vol. 26, no. 1, pp. 1–12, 2011.
[11] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, 2011.
[12] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. on Inf. Forensics and Security, vol.7, no.2, April, 2012.
[13] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, " Reversible data Hiding in encrypted images reserving room before encryption," IEEE Trans. On Inf. Forensics and Security vol. 8, no. 3, March, 2013.
[14] Image data base[online]. Available: http//sipi.use.edu /database/.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY