Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

AN ENHANCED SEPARABLE REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES USING SIDE MATCH

Mr. Khajavali Shaik[1] , Mr. Muzammil Parvez[2] M.Tech.,(Ph.D)
PG Scholar, Communications & Signal Processing[1], Assistant Professor[2]
[1,2]Nimra College of Engineering & Technology, Ibrahimpatnam

Abstract- This paper proposes a scheme for Enhanced Separable Reversible Data Hiding in Encrypted images Using Side Match. In the first step the original image is encrypted using an encryption key. Then additional data is embedded into the image by modifying a small portion of the encrypted image using a data hiding key. With an encrypted image containing additional data, if a receiver has the data hiding key, he can extract the additional data. If the receiver has the encryption key, he can decrypt the image, but cannot extract the additional data. If the receiver has both the data hiding key and encryption key, he can extract the additional data and recover the original content by exploiting the spatial correlation in natural images. The accuracy of data extraction is improved by using a better scheme for measuring the smoothness of the received image, and uses the Side Match scheme to further decrease the error rate of extracted bits.
Keywords: Encrypted image, reversible data hiding, smoothness, data extraction, side match.

I.INTRODUCTION

In recent years, signal processing in the encrypted domain has attracted considerable research interest. As an effective and popular means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. However, in some scenarios that a content owner does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired. For instance, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource.

II.EXISTING METHOD

Reversible Data Hiding in images is a technique that embeds data in digital images by altering the pixel values for secret communication, and the embedded image can be recovered to its original state after the extraction of the secret data. Many reversible Data Hiding methods have been proposed recently. One method embeds data bits by expanding the difference of two consecutive pixels. Another one uses a lossless compression technique to create extra spaces for carry data bits. Another method shifts the bins of image histograms to leave an empty bin for data embedment. Another one adopts the difference expansion and histogram shifting for data embedment. Another one embeds data by shifting the histogram of prediction errors while considering the local activity of pixels to further enhance the quality of stego-image.

Other applications could be for when the owner of the carrier might not want the other person, including data hider, to know the content of the carrier before Data Hiding is actually performed, such as military images or confidential medical images. In this case, the content owner has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded message and recover the original image. For example, our method encrypts the cover image before embedding is actually performed. The cover image is encrypted by applying bitwise exclusive-or (XOR) operator to every bit of pixels using an encryption key. Let be an 8-bit cover image of size W*H and Ii, j be the pixel value at (i, j).

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

Figure1. Four test images (a)Lena (b) Baboon (c)Sailboat (d)Splash

We denote the 8-bit binary digits of Ii,j as Ii, j(0) ,Ii, j(1) …Ii, j(7) ,where

$$I_{i,j}^{(k)} = \left[Ii, j \Big/ 2^{k} \right] \bmod 2, 0 \leq k \leq 7$$

To encrypt the cover image, a random sequence of size W*H*8 is generated using an encryption key:

$$r = \{ r_{i,j}^{(k)} \mid r_{i,j}^{(k)} \in \{0, 1\} \}_{k=0}^{7}, \; 0 \leq i \leq w\text{-}1, \; 0 \leq j \leq h\text{-}1.$$

Let $H^{m,n}$ is the block at position (m, n) of the partitioned blocks. According to a data-hiding key, data hider randomly and evenly classifies pixels in each block into sets S0 and S1. If the bit to be embedded in this block is "0", flip 3 LSBs of pixels in set S0; Let the flipped results be $H'^{m,n}$, where

$$H'^{m,n(k)} = \overline{H\, m,n\,(k)}, \; (u, v) \in S_0, \; k=0, 1, 2\ldots$$

On the contrary, if the bit to be embedded is "1," flip 3 LSBs of pixels in set S1, and the flipped result is

$$H'^{m,n(k)} = \overline{H\, m,n\,(k)}\,, (u, v) \in S_1, \; k=0, 1, 2\ldots$$

In above equations, $\bar{x}$ denotes the bit-flipping result of $H^{m,n}$ and $H'^{m,n}$ represent the k^{th} LSB of pixels at position (u, v) in blocks $H^{m,n}$ and $H'^{m,n}$, respectively. Repeat this process until all the data bits are embedded. The embedded and encrypted image is defined as *I"*.

To extract the embedded data bits, the random sequence is generated using the encryption key, and calculates the XOR of and the binary digits of *I"* to decrypt the image. The five MSBs of each pixel of the decrypted image will be identical to those of the cover image. According to the data-hiding key, pixels in sets S0 and S1 of each block are obtained. For block, $H'^{m,n}$ flip three LSBs of pixels in set S0 and calculate the XOR of the resultant bit stream and *r*, we obtain a block $H''^{m,n}$. Similarly, flip 3 LSBs of pixels of set S1 and calculate the XOR of the resultant bit stream *r* and, we obtain a block $\hat{H}^{m,n}$. Either $\tilde{H}^{m,n}$ or $\hat{H}^{m,n}$ is identical to the original block $H^{m,n}$, and the other one will be the block with three LSBs of every pixels flipped. Because the pixels are de-

correlated in the flipped blocks, the original blocks often exhibit smoother than those of flipped blocks. By comparing the smoothness of these two blocks, the embedded bits can be extracted. Smoothness calculation in existing method is

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

Where $p_{u,v}$ denotes the pixel value at position *(u, v)*, $|x|$ is the absolute value of x. Let the calculated smoothness of $\tilde{H}^{m,n}$ and $\hat{H}^{m,n}$ be $\tilde{f}^{m,n}$ and $\hat{f}^{m,n}$ respectively. If $\tilde{f}^{m,n} < \hat{f}^{m,n}$, a bit "0" is extracted, and $\tilde{H}^{m,n}$ is the original block. Otherwise, a bit "1" is extracted, and $H^{m,n}$ is the original block

In our method the border pixels of blocks are included in the process of smooth calculation. Moreover, the correlations between blocks are also considered in data extraction. These two facts could be exploited to enhance the correctness of extracted data. This method proposes a new smooth-evaluation function that fully exploits the pixels in blocks for evaluating the pixel fluctuations in images. A side-match mechanism is also introduced to evaluate the smoothness of those ambiguous blocks, where the absolute difference between and are smaller than a predefined threshold. With these sophisticated approaches, the correctness of data extraction will be further increased.

III.PROPOSED METHOD

In [9], the evaluation of block smoothness is crucial for obtaining a correct data extraction. However, the four borders of each block do not join the calculation of block smoothness. This may decrease the rate of correctness of data extraction, especially when the block size is small. For example, for a block of size 8X8, there are 64 pixels and around 43.75% of them (28 pixels) are located in the four borders. These border pixels are not employed to calculate the block smoothness, and the percentage is increased as the block size decreased. Besides, [9] extracts the embedded bits by evaluating the smoothness of a single block. However, flipping 3 LSBs of these complex blocks will not cause a significant increase in complexness. Based on these observations, this letter proposes an improved version for a better estimation of block smoothness. In the new smoothness estimation, the summation of the absolute of two neighboring pixels is employed. Moreover, the extraction and recovery are performed starting from the most noticeable changes in smoothness to the least ones. Besides, we also adopt the side-match technique to evaluate the block smoothness by concatenating the border of recovered blocks to the unrecovered blocks. The data encryption and data embedding process is the same as [9]. Therefore, we address only the calculation of smoothness and the process of image recovery.

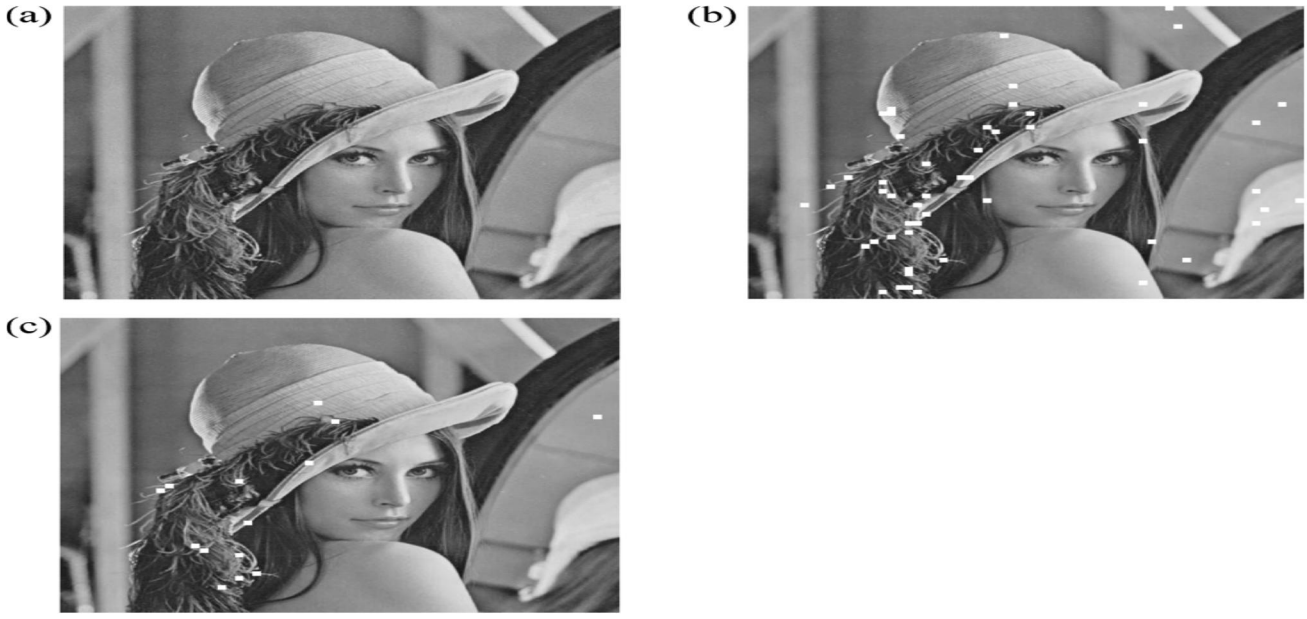

Figure2. (a) Decrypted image using content owner's key. (b) Blocks of incorrect recovery of Zhang's method. (c) Blocks of incorrect recovery of the proposed

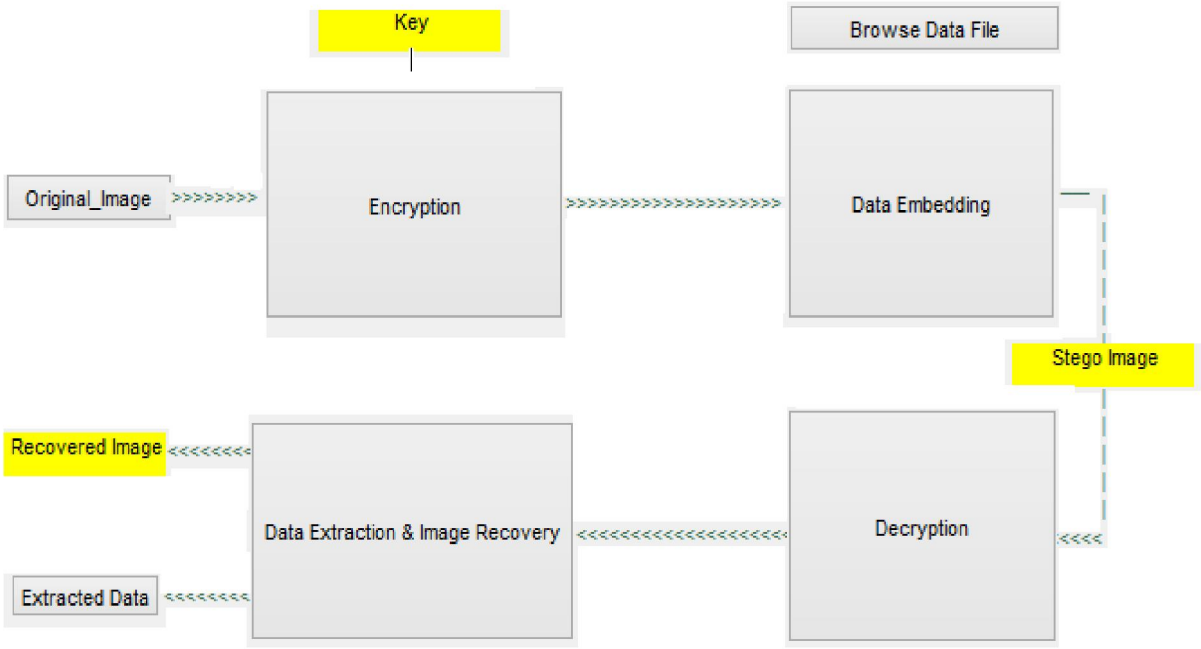

Figure3. Block diagram of proposed method

A.CALCULATION OF BLOCK SMOOTHNESS

The smoothness of an image block can be evaluated by calculating the absolute difference of neighboring pixels. The larger the summation of absolute differences, the more complex the image blocks is. Therefore, we estimate the block smoothness by calculating the summation of the vertical absolute differences and horizontal absolute differences of pixels in image blocks using the following equation:

$$f = \sum_{u=1}^{s2} \sum_{v=1}^{s1-1} (|p_{u,v} - p_{u,v+1}|) + \sum_{u=1}^{s2-1} \sum_{v=1}^{s1} (|p_{u,v} - p_{u+1,v}|)$$

Where $p_{u,v}$ represents the pixel values located at position of (u, v) a given image block of size $S_1 * S_2$ .Above Equation fully exploits the absolute difference between two consecutive pixels in both vertical and horizontal directions and thus, the smoothness of blocks can be better estimated.

B. DATA EXTRACTION AND IMAGE RECOVERY USING SIDE MATCH

Let the cover image be and the encrypted image with messages embedded be *I"*. Firstly, a random sequence is generated using the encryption key. The XOR of the 5 MSBs of *I"* and r are calculated to recover the five MSBs of the cover image. According to the data hiding key, the pixels in sets S0 and S1 of block $H'^{m,n}$ are obtained. Flip the three LSBs of pixels in set S0, and calculate the XOR of the resultant bit string and r, we obtain $\tilde{H}^{m,n}$. Similarly, flip the three LSBs of pixels in set, and calculate the XOR of the resultant bit string and, we obtained $\hat{H}^{m,n}$, above equation is then applied to evaluate the smoothness of $\tilde{H}^{m,n}$ and $\hat{H}^{m,n}$, and to obtain the evaluated results $\tilde{f}^{m,n}$ and $\hat{f}^{m,n}$, respectively. The difference $A^{m,n}$ between $\tilde{f}^{m,n}$ and $\hat{f}^{m,n}$ is obtained by the following equation

$$A^{m,n} = \tilde{f}^{m,n} - \hat{f}^{m,n}$$

A larger $|A^{m,n}|$ indicates that $H^{\sim m,n}$ is more dissimilar to $H^{\wedge m,n}$, which implies that the block $H^{m,n}$ becomes more complex after flipping 3 LSBs. Therefore, we calculate $|A^{m,n}|$ for all blocks, and sort $|A^{m,n}|$ in descending order. The data extraction and image recovery of blocks is then preformed using the sorted order of $|A^{m,n}|$.

IV. EXPERIMENTAL RESULTS

We used four gray level images of size 512x12, including Lena, Baboon, Sailboat, and Splash as the test images, as shown in Fig. 1. These images can be obtained from USC-SIPI image database [11]. The experimental results are compared with [9].

To demonstrate the performance of the proposed method, we take Lena image as an example. Fig. 2(a) shows the decrypted Lena image with 5 MSBs recovered (suppose the block size is 8X8). Figs. 2(b) and (c) show the recovery results using [9] and the proposed method, respectively, where the incorrect recovered blocks are marked by white. Note that most of the incorrect recovered blocks are sparsely distributed over the complex regions of the Lena image. Comparing Figs. 2(b) and (c), we see that the proposed method recovers the image blocks more accurate than that of [9]. Although the experiments were based on Lena image, experiments on other test images also showed the proposed method effectively improves Zhang's method, especially when the block size is small.

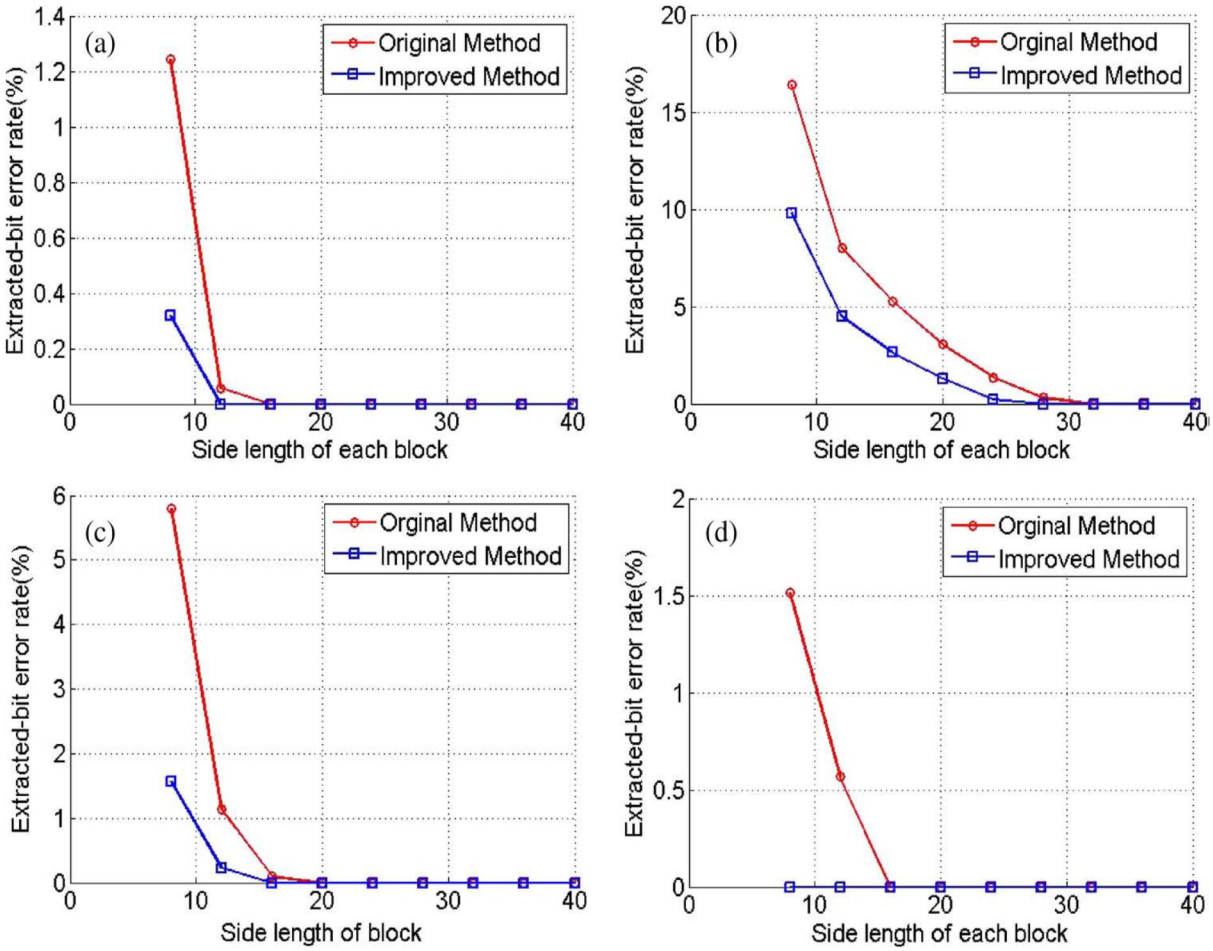

Fig. 3. The error rate comparison. (a) Lena. (b) Baboon. (c) Sailboat. (d) Splash.

V. CONCLUSION

This paper proposes a scheme for Enhanced Separable Reversible Data Hiding in Encrypted images Using Side Match. We used a new algorithm to better estimate the smoothness of image blocks. The extraction and recovery of blocks are performed according to the descending order of the absolute smoothness difference between two candidate blocks. The side match technique is employed to further reduce the error rate. The experimental results show that the propose method effectively improves Zhang's method, especially when the block size is small

VI. REFERENCES

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

[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, andW. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 8, pp. 354–362, 2006.

[4] 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.

[5] 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.

[6] D.Kundur andK.Karthik, "Video fingerprinting and encryption principles for digital rights management," Proc. IEEE, vol. 92, pp. 918–932, 2004.

[7] 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.
[8] 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.
[9] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, 2011.
[10] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, 10.1109/TIFS.2011.2176120.
[11] Image database [Online]. Available: http://sipi.use.edu/database/

