A Secure Data Hiding Scheme Using RIDH over Encoded Domains

A. Sandhya Lakshmi[1], J. Vamsinath[2]
[2]M.Tech, Dept. of CS, PBR Visvodaya Institute of Technology and Science, AP, India.
[1]Dept. of CS, PBR Visvodaya Institute of Technology and Science, AP, India.

***Abstract*:**

Objective: This paper is aimed to study the data hiding technique using RIDH over encrypted domain.

Methods/Statistical analysis: In recent surveys show the different data hiding mechanisms in non encrypted domains. But still there is gap in applying the data hiding techniques in encrypted domain. To fulfil this gap, we propose a novel **reversible image data hiding (RIDH)** scheme over encrypted domain. The data embedding is achieved through a public key modulation mechanism, in which access to the secret encryption key is not needed. At the decoder side, a powerful two-class SVM classifier is designed to distinguish encrypted and non-encrypted image patches, allowing us to jointly decode the embedded message and the original image signal.

Findings: To evaluate the efficiency of our proposed work, we compared with the state-of-the-arts, the proposed approach provides higher embedding capacity, and is able to perfectly reconstruct the original image as well as the embedded message. Extensive experimental results are provided to validate the superior performance of our scheme.

Applications/Improvements: we collect the test dataset which includes 100 images with size of 512 x 512. All these images are downloaded from the following link https://dl.dropboxusercontent.com/u/103270026/TestImage.zip.

Keywords: Data Hiding, public key modulation, SVM, Signal processing.

1. Introduction

Reversible image data hiding (RIDH) is an uncommon classification of information hiding strategy, which guarantees ideal reproduction of the cover picture upon the extraction of the embedded message. The reversibility makes such picture information hiding methodology especially appealing in the basic situations, e.g., military and remote sensing, medical pictures sharing, law legal sciences and copyright verification, where high constancy of the reproduced cover picture is required.

Most of the current RIDH algorithms are structured over the plaintext, to be specific, the message bits are embedded into the first, un-encoded pictures. The early works for the most part used the lossless compression algorithm to compact certain picture features, so as to reduce space for message embedding[1, 2]. Notwithstanding, the embedded limit of this kind of technique is fairly restricted and the acquired distortion on the watermarked picture is extreme. Histogram shifting (HS)- based method, at first developed by Ni et al.[3], is another class of methodology accomplishing better embedding efficiency through shifting the histogram of some picture features[4,5]. The most recent different extension (DE)- based plans and the enhanced prediction error expansion (PEE)- based techniques were appeared to have the capacity to offer the best in class capacity distortion performance[6-10].

As of late, the exploration on signal processing over encoded domain has increased expanding consideration, basically determined by the necessities from Cloud platforms and different protection safe applications[11-14]. This has set off the examination of embedding extra information in the encoded pictures in a reversible model. To ensure the protection and security, all pictures will be encoded before being sent to an un-trusted third party for further processing. For example, in secure remote detecting, the satellite pictures, after being caught by on-board cameras, are encoded and after that sent to the base station(s), as represented in Fig. 1. After getting the encoded pictures, the base station embeds a private message, e.g., base station ID, area data, time of arriving (TOA), surrounding temperature, wind speed, and so forth., into the encoded pictures.

Insert Figure 1 Here

Moreover, like the instance of Cloud processing, it is basically expensive to enforce a solid key Management System (KMS) in such multi-party context over insecure open systems, because of the distinctions in ownership and control of underlying environments on which the KMS and the ensured assets are located[15]. It is accordingly much wanted if secure information hiding could be accomplished without an extra screte information hiding key shared between the base station and the server. At long last, the server, which has abundant computing assets, removes the embedded message and extract the original picture by utilizing the encryption key K.

In this work, we propose a Encrypted-domain RIDH mechanism by explicitly taking the previously mentioned structure preferences into mind. The proposed procedure embeds message through an public key system, and performs information extraction by misusing the measurable distinguishability of encoded and non-encoded picture parts. Since the decrypting of the message bits and the original picture is integrated, our proposed strategy has a place with the classification of non-distinct RIDH solutions[16]. Compared with the state-of-the-arts, the proposed methodology gives higher embedding limit, and can accomplish ideal reproduction of the original picture and additionally the embedded message bits. Evalution results on 100 test pictures approve the high efficiency of our plan.

2. Research Method

Rather than considering best encoded algorithms customized to the situation of encoded-domain information hiding, we here adhere to the regular stream cipher applied in the standard organization. That is, the ciphertext is created by bitwise XORing the plaintext with the key stream. If not generally indicated, the broadly utilized stream cihper AES in the CTR mode (AESCTR) is expected. The subsequent information hiding worldview over encoded domain could be all the more basically valuable due to two reasons: 1) stream cipher utilized in the standard format, is as yet a standout amongst the most famous and dependable encoded tools, because of its provable security and high programming/equipment usage efficiency[17]. It may not be simple, or even infeasible, to influence clients to receive new encoded algorithms that have not been altogether assessed; 2) vast number of information have just been encoded utilizing stream cipher standardly.

At the point when stream cipher is utilized, the encoded picture is created by

$$[[f]] = Enc(f, K) = f \oplus K \qquad (1)$$

In this work, without loss of generality, every one of the pictures are thought to be 8-bit. All through the paper, we utilize $[[x]]$ to speak to the encoded form of x. Unmistakably, the original picture can be acquired by performing out the accompanying decoding capacity

$$f = Dec([[f]], K) = [[f]] \oplus K \qquad (2)$$

The schematic graph of the proposed message embedding algorithm over encoded domain is figured in Fig. 2. In this work, we do not think about the instance of embedding various watermarks for one single part, implying that each part is handled once at most. For effortlessness, we accept that the quantity of message bits to be embedded is $n.\ A$, where $A \leq B$ and B is the quantity of parts inside the picture. The means of playing out the message embedding are summerized as pursues:

1. Initialize block index $i = 1$.
2. Extract n bits of message to be embedded, indicated by W_i.
3. Find the public key $Q_{[W_i]d}$ related with W_i, where the index $[W_i]_d$ is the decimal representation of W_i. For instance, when n = 3 andW_i = 010, the corresponding public key is Q_2.
4. Embed the length-n message bits W_i into the ith block via

$$[[f]]_i^w = [[f]]_i \oplus Q_{[W_i]d} \qquad (3)$$

Step 5: Increment i = i + 1 and repeat Steps 2-4 until all the message bits are inserted.

Insert Figure 2 Here

The watermark length parameter A should be transmitted alone with the installed message bits. There are numerous approaches to take care of this issue. For example, we can hold a few parts to insert A. Or on the other hand, we can attach a finish of-document symbol to the message to be inserted, to such an extent that the decoder can certainly decide A.

From the above steps, it very well may be seen that the message inserting is performed without the guide of a private information hiding key. This area demonstrated high level of inserting security can in any case be ensured, on account of the assurance offered by the encoded key K. Likewise, the calculations engaged with message inserting are somewhat tiny (basic XOR activities), and all the part-by-part preparing can be promptly made parallel, accomplishing high-throughput.

It is stressed that the likelihood of removing out the information hiding key is not one of a kind to our proposed strategy, yet rather arguably applicable for all non-distinct RIDH plans over encoded domain.

In other words, the security scheme in the encoded domain can be normally stretched out to give security to message embedding, taking out the need of presenting an additional information hiding key. This could prompt huge decrease of the computational expense and potential danger of working up a safe KMS, which has been ended up being extremely testing in the multi-party environment[15].

3. Result and Analysis

In this segment, we tentatively test the embedding efficiency of our proposed encoded domain RIDH plan. The test set is made out of 100 pictures of size 512 × 512 with different attributes, including normal pictures, engineered pictures, and exceptionally finished pictures. All the test pictures can be downloaded from https://dl.dropboxusercontent.com/u/103270026/TestImage.zip. Clearly, the test set is not quite the same as the training set utilized to infer the two-class SVM classifier.

We stick to uniform encoded strategy, and every one of the pictures is encoded utilizing the stream cipher AES-CTR[16]. We might want to contrast our plan and three best in class algorithms[18-20], where standard encoded strategies were additionally utilized. Here, τ is characterized by

$$\tau = \frac{\#\ of\ correctly\ extracted\ bits}{\#\ of\ embedded\ bits} \qquad (4)$$

and the values given are average of over all the parts in the 100 test pictures. As the plan of[18] just chips away on parts no under 3×3, the outcomes for littler part designs are set apart with '– '. For reasonable correlation with[18-19], we attempt diverse quantities of flipped LSBs, rather than settling to flip 3 LSBs, and just record the best extraction precision.

This is comparable to expel the imperative on direct decoding. It very well may be seen that, for all the three techniques, the embedding capacity increments as the block size drops. Our technique can insert 21675 message bits for each 512×512 picture when the part size is 6×6, while guaranteeing 100% exactness of information extraction. As the part size declines further, modest number of extraction mistakes appears. Notwithstanding, when the part size shrinks to 2×2, the exactness is still as high as 99.2356%. Conversely, the estimations of τ[18] and its enhanced version[19] are reliably lower than 100%, notwithstanding when the part size is as large as 8 × 8. Likewise, for a similar part size, the extraction exactness of our technique is altogether higher than those of[18-19] while the embedded capacity is multiple times higher.

In addition to the comparison of the averaged extraction accuracy, we also show the results of these three methods for six representative images illustrated in Fig. 3. As can be seen from Fig. 4, for images with large portion of textural regions, e.g., Texture mosaic 1 and Cactus,[18, 19] give much degraded results, especially when the block size is small.

In addition to the correlation of the averged extraction exactness, we demonstrate the three techniques for six pictures showed in Fig. 3. As can be seen from Fig. 4, for pictures with vast segment of textural locales, e.g., Texture mosaic 1 and Cactus,[18, 19] give much debased outcomes, particularly when the part size is tiny.

Insert Figure 3 Here

Insert Figure 4 Here

Finally, we evaluate the time complexity of performing the joint decryption and data extraction, with respect to different settings of n, where n is the number of bits embedded into one single block. The computational complexity mainly comes from applying SVM classifier to the $S = 2^n$ decoding candidates. Since the SVM training is conducted off-line, the associated complexity will not be counted into the evaluation of joint decryption and data extraction. In Fig. 5, the results are averaged over all the 100 test images of size 512 × 512.

At last, we evaluate the time complexity of playing out the joint decoding and information extraction, as for various settings of n, where n is the quantity of bits inserted into one single block. The computational complexity comes from applying SVM classifier to the $S = 2^n$ decoding blocks. Since the SVM training is performed in off-line, the related intricacy will not be checked into the evaluation of joint decoding and information extraction. In Fig. 5, the outcomes are averged over all the 100 test pictures of size 512 × 512.

Insert Figure 5 Here

4. Conclusion

In this paper, we plan a secure reversible image data hiding (RIDH) conspire worked over the encoded domain. We recommend an public key system, which enables us to embedd the information by means of straightforward XOR activities, without the need of getting to the secrete encoded key. At the decoder side, we propose to utilize an amazing two-class SVM classifier to separate encoded and non-encoded picture patches, empowering us to jointly decode the embedded message and the original picture signal exactly. We also performed broad examinations to approve the higher embedding efficiency of our proposed RIDH technique over encoded domain.

References

1. M. U. Celik, G. Sharma, A. Tekalp, and E. Saber,“Lossless generalizedlsb data embedding,” IEEE Trans. Image Process., vol. 14, no. 2, pp.253-266, 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, 2006.

3. Z. Ni, Y. Shi, N. Ansari, and W. Su,“Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354-362, 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 Secur, vol. 8, no. 7, pp. 1091-1100, 2013.

5. C. Qin, C.-C. Chang, Y.-H. Huang, and L.-T. Liao,“An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism,” IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 7, pp. 1109-1118, 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, 2009.

7. J. Tian,“Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, 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, 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, 2011.

10. X. Zhang,“Reversible data hiding with optimal value transfer,” IEEE Trans. Multimedia, vol. 15, no. 2, pp. 316-325, 2013.

11. T. Bianchi, A. Piva, and M. Barni,“On the implementation of the discrete fourier transform in the encrypted domain,” IEEE Trans. Inf. Forensics Secur., vol. 4, no. 1, pp. 86-97, 2009.

12. T. Bianchi, A. Piva, and M. Barni,“Composite signal representation for fast and storage-efficient processing of encrypted signals,” IEEE Trans. Inf. Forensics Secur., vol. 5, no. 1, pp. 180-187, 2010.

13. M. Barni, F. P., R. Lazzeretti, A.-R. Sadeghi, and T. Schneider,“Privacypreserving ecg classification with branching programs and neural networks,” IEEE Trans. Inf. Forensics Secur., vol. 6, no. 2, pp. 452-468, 2011.

14. Z. Erkin, T. Veugen, T. Toft, and R. Lagendijk,“Generating private recommendations efficiently using homomorphic encryption and data packing,” IEEE Trans. Inf. Forensics Secur., vol. 7, no. 3, pp. 1053-1066, 2012.

15. M. Chandramouli, R. Iorga and S. Chokhani,“Cryptographic key management issues and challenges in cloud services,” NIST Report 7956, pp. 1-31, 2013.

16. X. Zhang,“Separable reversible data hiding in encrypted image,” IEEE Trans. Inf. Forensics Secur., vol. 7, no. 2, pp. 826-832, 2012.

17. H. Lipmaa, P. Rogaway, and D. Wagner,“Ctrmode encryption,” [Online] Available: http://csrc.nist.gov/encryption/modes/workshop1/papers/lipmaa-ctr.pdf.

18. X. Zhang,“Reversible data hiding in encrypted image,” IEEE Signal Processing Lett., vol. 18, no. 4, pp. 255-258, 2011.

19. T. Hong, W. Chen and H. Wu,“An improved reversible data hiding in encrypted images using side match,” IEEE Signal Processing Lett., vol. 19, no. 4, pp. 199-202, 2012.

20. W. Puech, M. Chaumont, and O. Strauss,“A reversible data hiding method for encrypted images,” in Proc. of SPIE 6819, 2008, pp. 1-9.

Figures

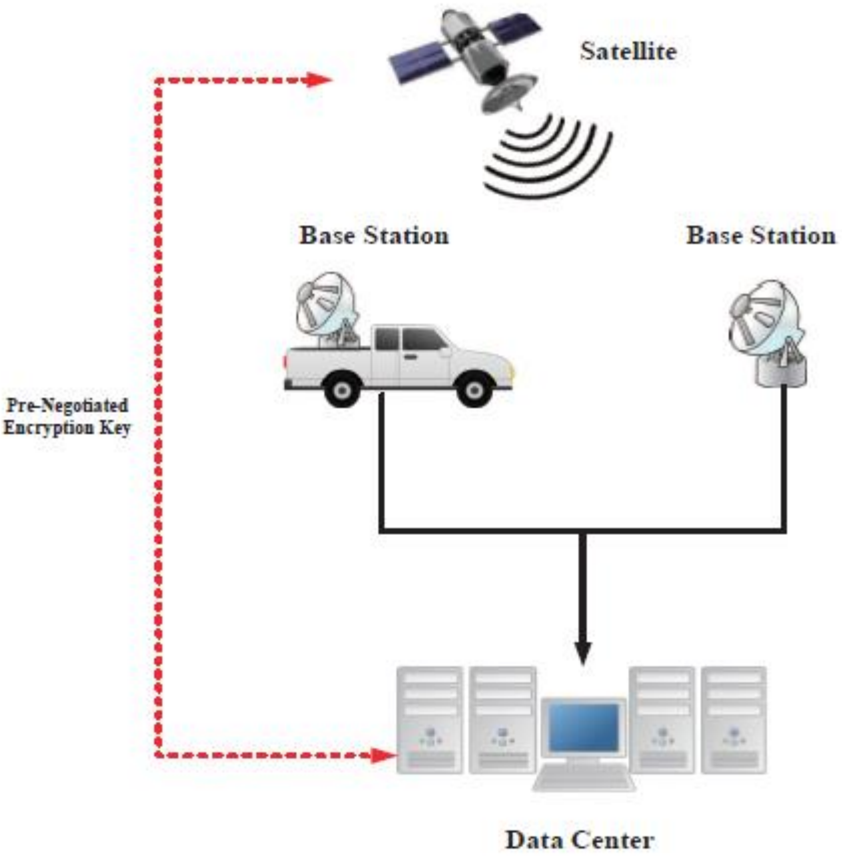


Fig. 1: Image data hiding in the scenario of secure remote sensing.

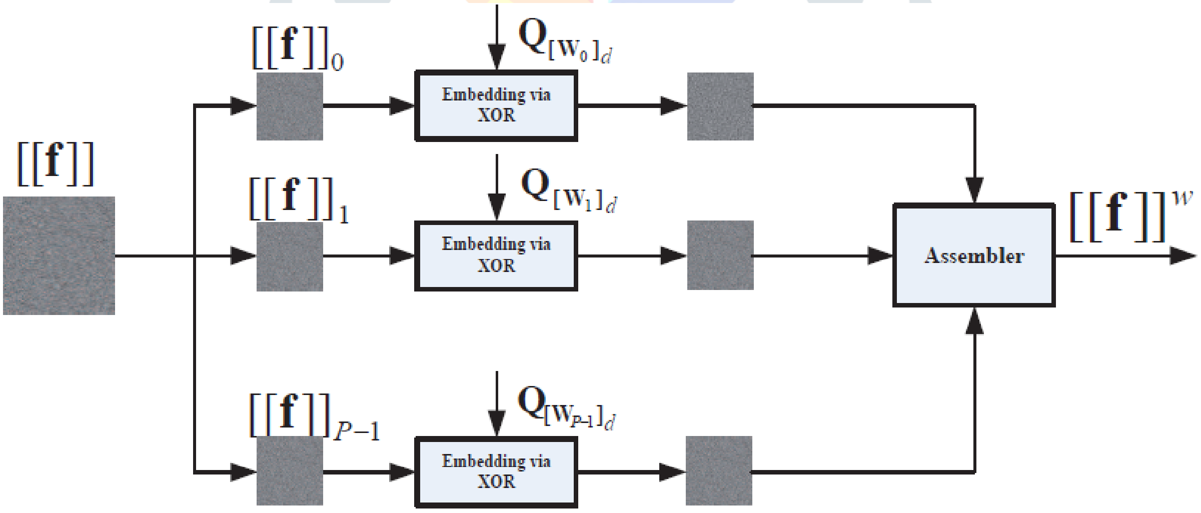
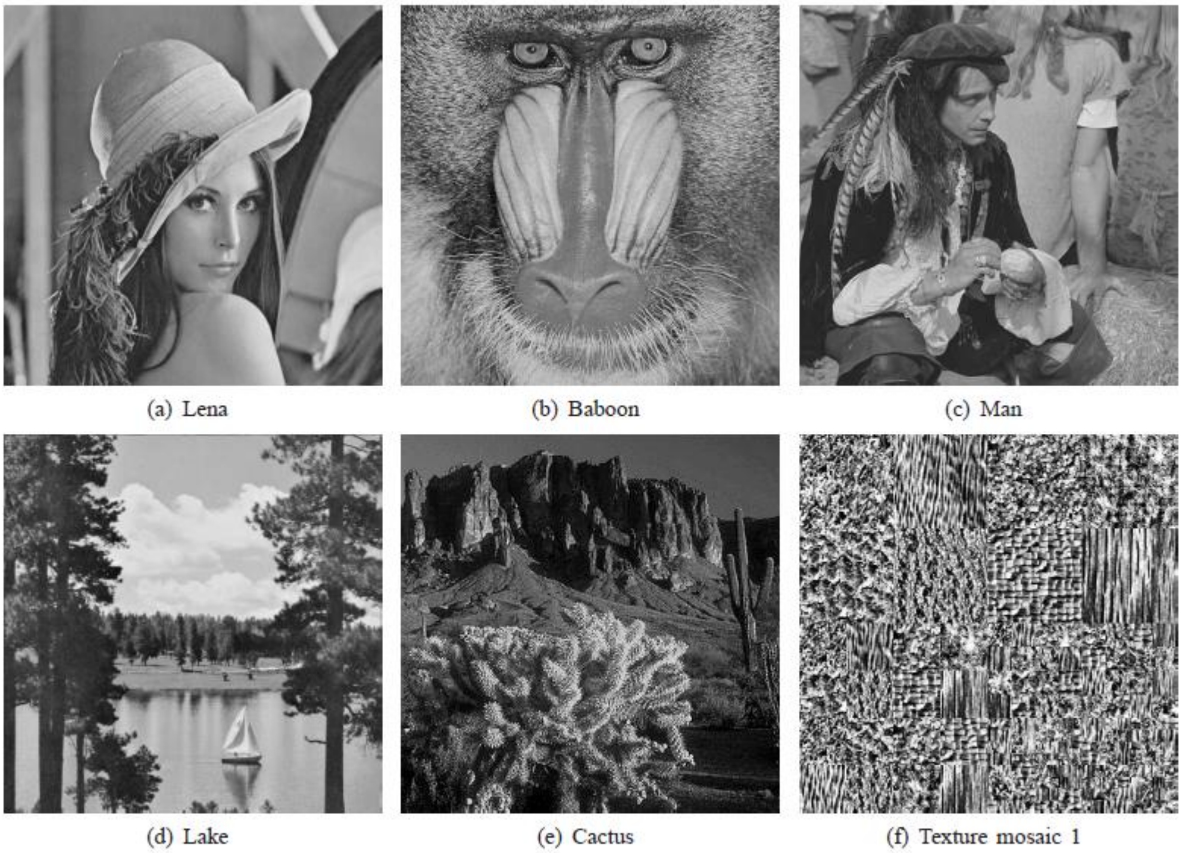


Fig 2: Schematic diagram of data hiding over encrypted domain.



(a) Lena (b) Baboon (c) Man

(d) Lake (e) Cactus (f) Texture mosaic 1

Fig.3: Six test images for fine-grained comparison.

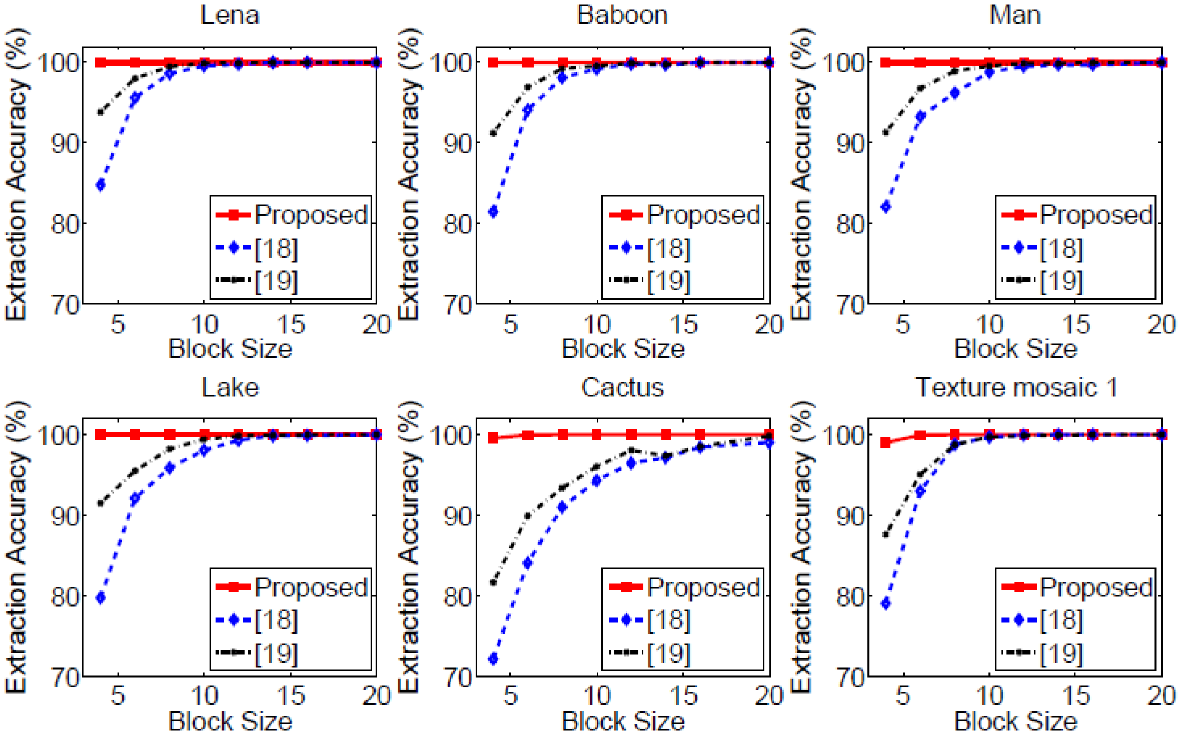


Fig. 4: Comparison of the extraction accuracy for six representative test images.

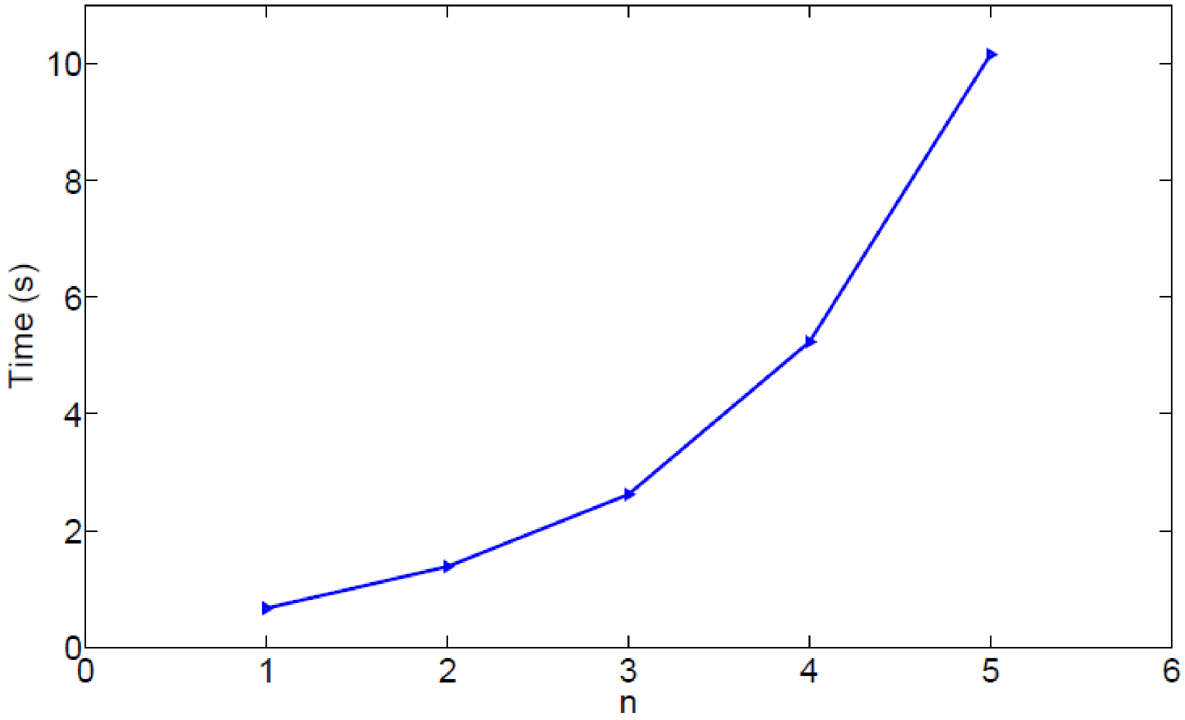


Fig. 5: Time complexity of performing the joint decryption and data extraction over an un-optimized, un-paralleled Matlab implementation.