Mathematical Statistician and Engineering Applications
ISSN: 2326-9865
DOI: https://doi.org/10.17762/msea.v70i1.2309

Hiding the Data Using Hybrid of LSB and AES in Encrypted Image

Purushottam Das

Asst. Professor, Department of Computer Science, Graphic Era Hill University, Dehradun, Uttarakhand India 248002

Article Info
Page Number: 277-284
Publication Issue:
Vol. 70 No. 1 (2021)

Abstract
In this technique, which is known as "Reserving Room before Encryption," we first allotted some space for data embedding. Then, the picture was encrypted using the private key, which helps to safeguard the encryption process. Using a different private key, the data is then securely hidden in an encrypted image. Following points, we receive two private keys from the transmitter side, which increased the encryption and decryption processes' security. The data hiding the encrypted image and the two private keys are now sent to the receiver. Receivers can only retrieve data and images if they have access to the encryption key and the data concealing private key, respectively. Thus, the image and data were not easily recovered by the hackers. Because of this, despite the AES algorithm's mathematical soundness, the primary underlying issues with it, like as speed and the use of subpar or tiny prime integers that have resulted in severe security breaches, may be resolved. A basic and commonly utilised technology worldwide is public key cryptography. The majority of public key algorithms, including AES, are based on modular arithmetic. As a result, performing public key encryption and decryption requires performing several modular multiplications on very large values. As a result, symmetric key algorithms are known to be faster than public key algorithms. It has recently become increasingly commonplace to use GPUs for general-purpose computing. The extremely parallel features have been used to significantly improve the performance of many computer problems.

Article History
Article Received: 25 January 2021
Revised: 24 February 2021
Accepted: 15 March 2021

1. Introduction

In the emerging world, security is more crucial. It was easily hackable by the hacker during data transmission. Knowing the dates' secrets is helpful. One of the earliest methods of sending secret data is called steganography and involves disguising the data in a picture. In order to improve the security of software systems employing the AES algorithm and its performance, this article offers the idea and implementation of the method. We studied the AES algorithm for this paper. This research explains the AES algorithm and the rationale behind its usage in network security and cryptography. After conducting a number of studies on the subject, we came to the conclusion that the AES algorithm is crucial for network security because it contains components (such as encryption and decryption keys) that communicate with the security system. AES is a technique for reversibly concealing extra data within a cover media. The cover media must be restored without distortion and the data must be extracted without mistakes. AES techniques have advanced significantly over the past 20 years, giving rise to complex algorithms with large embedding capacities and little cover distortion. Looking deeper into the past, one of the first AES advancements may be linked to a 1994 patent application made by Barton.

By including an unnoticeable digital signature into the digital material, this invention offers a method and equipment for authenticating it. An authorised individual can use the digital signature to recover the content and demonstrate its originality.

The two most crucial points in this work are that public key cryptography is a basic and commonly used technology worldwide and that public key encryption and decryption are computationally intensive owing to the numerous modular multiplications with extremely big numbers required to carry out these activities. The subject of employing GPUs for general-purpose computing has recently increased in popularity, and by utilising the highly parallel features, many computational issues have seen a large performance boost. This technique can address the primary underlying issues with the AES algorithm, such as speed and the use of suboptimal or tiny prime numbers that have resulted in severe security flaws. Public key encryption and decryption are computationally intensive because they need many modular multiplications with very big numbers, which is a basic and extensively utilised technology worldwide.

2. Literature Survey

An innovative approach of reversible data embedding for digital photographs is presented in this research. To obtain a very high embedding capacity and minimise distortion, it investigates the redundancy in digital pictures. The Barton patent, submitted in 1994, contains the first mention of reversible data embedding. For lossless image recovery, Honsinger et al. rebuild the payload from an embedded picture before subtracting the payload from the embedded image. To accomplish reversible data embedding, Macq suggests extending the patchwork approach. A large capacity reversible data-embedding method based on message embedding on bits in the state of a set of pixels is developed by Fridrich et al. A reversible data-embedding technique using circular interpretation of bijective transformations is proposed by De Vleeschouwer et al. In addition to offering a useful code design, Kalker et al. discuss some theoretical capacity limitations of lossless data compression based reversible data embedding. The G-LSB approach includes numerous implementations, however Celik et al. find that the selective embedding extension performs best in terms of capacity versus distortion. The DE technique, the G-LSB strategy, & the RS method on "Lena" are compared for capacity and distortion [1].

This study introduces a unique reversible (lossless) data concealing (embedding) method that, upon extraction of the embedded data, allows precise recovery of the original host signal. It offers a generalisation of the LSB (least significant bit) modification technique, which adjusts the host signal's lowest levels to make room for the payload data. The capability for lossless data embedding increases with the use of a prediction-based conditional entropy coder. High lossless embedding capacity can only be achieved with effective residual compression. A brand-new method of embedding (hiding) lossless data is provided that has large embedding capacities, fully restores the original host signal, and adds only a minor amount of distortion between the host and the picture that contains the embedded data. Benefits include the generalised LSB embedding suggested in the current research and the direct use of the G-LSB embedding technique for low distortion data embedding. The host signal's digital

representation has a small range of possible values, which might cause issues, and the rate of rise is not consistent [2].

Reversible picture watermarking allows for the loss-free insertion of valuable or copyright information in a host image. This study suggests a unique method for enhancing embedding capacity by combining adaptive prediction error expansion with pixel selection. By separating the picture pixels into two parts with embedding 2 bits into the flat region and 1 bit into the rough region pixels, the suggested approach combines adaptive embedding with pixel selection. An effective reversible watermarking technique called adaptive prediction error expansion (PEE) embeds extra bits into expandable pixels found in flat areas. It picks pixels whose forward variances fulfil FV PS, where PS is a threshold, and can reach an ER of up to 1.8 BPP. Prediction-error expansion, which combines the benefits of expansion embedding with the greater de correlating skills of a predictor, embedded data in any picture, and permanently erasing information within changed pixels are some advantages [3].

Numerous significant multimedia applications use digital information and images embedding systems to place one signal—sometimes referred to as a "embedded signal" or "information"—within another signal, known as a "Host Signal." Reversible data hiding (AES) in encrypted pictures has received increasing attention recently because it preserves the exceptional characteristic that the original cover may be lostlessly reconstructed once embedded data is retrieved while protecting the privacy of the image content. This work suggests a narrative strategy that allows the data hider to reversibly embed data in the encrypted image without difficulty by making room before encryption with a normal AES algorithm. Additionally, it creates a framework that allows for the evaluation of information embedding method performance in terms of the rate-distortion-robustness trade-offs that can be achieved, and it explores how prior recommended data hiding algorithms suitable into this framework. This research suggests a unique way for AES in encrypted photos that "reserves room before encryption" rather than "vacates room after encryption" as is often done. This technique makes data concealing simple by letting the data hider utilise the excess space that was freed up in the earlier step. Benefits include good performance without compromising full secrecy, support from all conventional AES approaches for plain pictures, and excellent performance. Its limitations, including as the fact that it only works with binary images, and how it impacts image quality, are drawbacks [4].

Without losing host data, reversible watermarking makes it possible to incorporate helpful information in a host signal. Tian's difference-expansion approach for data embedding is high-capacity and reversible, however it suffers from distortion and lacks capacity management. An efficient technique for data embedding combines prediction-error expansion with histogram shifting. Although Tian's DE scheme employs multiple or recursive embedding, it does not fully take advantage of the correlation present in a neighbourhood. Alattar added a reversible embedding method for a generalised integer transform to the DE approach. A highly compressed overflow map and flag bits are used in one of the two brand-new reversible watermarking methods that were described. Prediction-error expansion has a larger capacity for data-embedding than DE because it combines the benefits of expansion embedding with a

predictor's stronger decorrelating skills. The requirement to incorporate the location map twice for payloads over 0.5 bpp disadvantages Algorithm D1 [5].

3. Proposed System

Use Reverse room before using encryption. In order to keep additional dates, enlarge the encrypted picture. Use Data is concealed in encrypted images using reversible data concealing techniques. Get two keys for two distinct processes. Currently, secret key encryption is done using the Advanced Encryption Standard (AES). In order to replace the outdated Data Encryption Standard (DES), two cryptographers from Belgium, Vincent Rijmen and Joan Daemen, developed AES. A standardised version of the Rijndael algorithm was utilised for the Advanced Encryption Standard under the Federal Information Processing Standard 197. The algorithm combines row and column rotations, a Mix Column, octet conversion with an S-box, Exclusive-OR operations (XOR), and octet substitution.

It worked well since it was simple to set up and took just a fair amount of time to complete on a typical computer. With a fixed block size of 128 and a configurable key length, AES is an iterated block cypher. The various transformations work on the state-designated intermediate outcomes. The state is a rectangular array of bytes with a block size of 128 bits, or 16 bytes, making the rectangular array 4 by 4 in size. (The row size is fixed at four while the number of columns vary in the Rijndael version with variable block size. By dividing the block size by 32, the number of columns (abbreviated Nb) is obtained. Similar representations of the cypher key include a rectangular array with four rows. The following benefits of the suggested strategy are listed:

- Even though the LSB technique was already utilised in the previous system, we used it in the proposed system to integrate a significant amount of data.
- Additionally, we have taken steps to lower the image's noise level after decryption. so that the output is highly accurate.

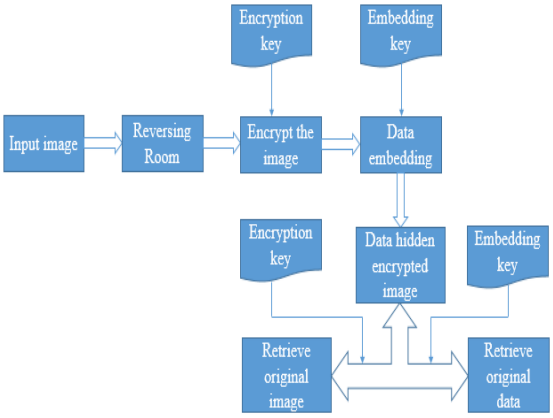

Fig 1: System Architecture

The next section provides an explanation of the many phases that are involved in putting the suggested technique into practice:

1. Preprocessing

Set aside space for storing images and data; this space will be determined by the sizes of the images and the data. Then put the image in the designated spot. Before an image is stored, its size must fit within the space allotted. The room for reservations in the image may be arranged according to the length of the data using the equation below.

$$f = \sum_{u=2}^{m} \sum_{v=2}^{N-1} \left| \mathbf{C}_{u,v} - \frac{\mathbf{C}_{u-1,v} + \mathbf{C}_{u+1,v} + \mathbf{C}_{u,v-1} + \mathbf{C}_{u,v+1}}{4} \right|$$

2. Image Encryption

Following storage in the designated space, the image was encrypted using the AES algorithm. The picture matrix's column and row values are changed based on the private key being generated throughout that procedure. Users provide the private key. The generate key is made by giving the picture depending on that size.

3. Data Hiding

After image encryption, the data is embedded in the encrypted image using a hybrid of the least significant bit (LSB) and the most secure encoding (AES), using a private key provided by the users. The encrypted image contains LSB values based on the space allotted to us.

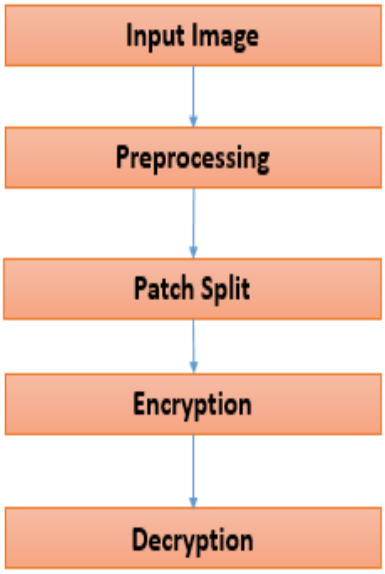

Fig 2: Flow Diagram

4. Image Decryption

The picture was first encrypted by the user and then decrypted using the generated key. It is the picture encryption process done backwards. The displaced columns and rows return to their original positions and retrieve the original picture. After then, the Data was kept in the designated place.

5. Data Extraction

After receiving the private data embedding key, the stored data was retrieved. The Data embedding procedure is in opposition to that one.

4. Results

Two Belgian cryptographers, Vincent Rijmen and Joan Daemen, created the Advanced Encryption Standard (AES), an iterated block cypher to replace the stale Data Encryption Standard (DES). Row and column rotations, a Mix Column, octet conversion with an S-box, Exclusive-OR operations (XOR), and octet substitution are all included in this method, which is straightforward to set up and takes just a moderate amount of time to execute on a standard computer. A customizable key length and a fixed block size of 128 characterise this iterated block cypher. Data security and secrecy may be achieved using an efficient method that combines LSB and AES encryption to hide data in encrypted pictures.

In addition, it adds a layer of protection that makes it more challenging for hackers to locate and extract the encoded data. To avoid data breaches, it is crucial to have many levels of protection. Overall, the LSB/AES encryption approach hybrid offers a trustworthy and effective way to conceal data in encrypted photos.

Fig 3: Filtered Image

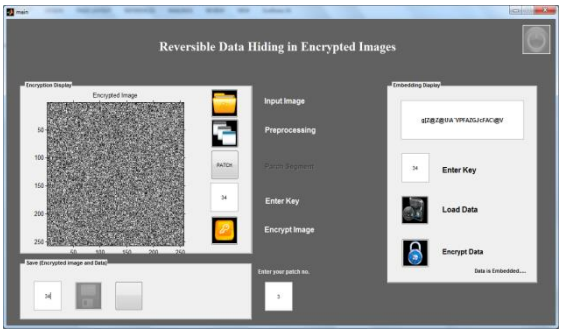

Fig 4: Encrypted Image

Fig 5: Image Decoding

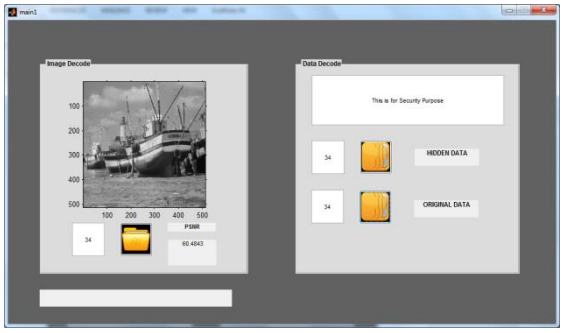

Fig 6: Data Decoding

5. Conclusion

In conclusion, the hybrid of LSB and AES encryption technique for hiding data in encrypted images is an effective approach for ensuring data security and confidentiality. The method allows for the efficient embedding of confidential information into the image while also ensuring the image's integrity and quality are maintained. The use of AES encryption ensures that the embedded data is protected with a strong encryption key, while the LSB technique allows for efficient data embedding. Furthermore, the hybrid technique provides an added layer of security, making it difficult for hackers to identify and extract the embedded data. This is because the data is not only encrypted but also hidden within the image, making it less visible to attackers. Additionally, the use of encrypted images provides an additional layer of protection, as unauthorized access to the image would not reveal the hidden data. However, it is important to note that no security method is foolproof, and attackers may still find ways to compromise the system. Therefore, it is important to implement multiple layers of security, including regular software updates, strong passwords, and user education to prevent data breaches. Overall, the hybrid of LSB and AES encryption technique provides a reliable and efficient method for hiding data in encrypted images, and its effectiveness has been demonstrated in various applications. As technology advances, it is important to continually improve and evolve security measures to ensure data remains secure and protected.

reference

1. Zhao, Gaochang, et al. "AES-based digital image encryption algorithm in wireless sensor networks." Signal Processing Systems (ICSPS), 2010 2nd International Conference on. Vol. 2. IEEE, 2010.

2. Chang, Chin-Chen, Min-Shian Hwang, and Tung-Shou Chen. "A new encryption algorithm for image cryptosystems." Journal of Systems and Software 58.2 (2001): 83-91.
3. Manavski, Svetlin A. "CUDA compatible GPU as an efficient hardware accelerator for AES cryptography." Signal Processing and Communications, 2007. ICSPC 2007. IEEE International Conference on. IEEE, 2007.
4. Nickolls, John, et al. "Scalable parallel programming with CUDA." Queue 6.2 (2008): 40-53.
5. Ryoo, Shane, et al. "Optimization principles and application performance evaluation of a multithreaded GPU using CUDA." Proceedings of the 13th ACM SIGPLAN Symposium on Principles and practice of parallel programming. ACM, 2008.
6. A. Redondi, M. Cesana, and M. Tagliasacchi, “Rate-accuracy optimization in visual wireless sensor networks,” in *Proc. 19th IEEE Int. Conf. Image Process.*, Orlando, FL, USA, Oct. 2012, pp. 124–129.
7. B. Tavli, K. Bicakci, R. Zilan, and J. Barcelo-Ordinas, “A survey of visual sensor network platforms,” *Multimedia Tools Appl.*, vol. 60, no. 3, pp. 689–726, 2012.
8. K. Obraczka, R. Manduchi, and J. J. Garcia-Luna-Aveces, “Managing the information flow in visual sensor networks,” in *Proc. 5th Int. Symp. Wireless Pers. Multimedia Commun.*, vol. 3. Honolulu, HI, USA, Oct. 2002, pp. 1177–1181.
9. S. Lee, S. Lee, and A. Bovik, “Optimal image transmission over visual sensor networks,” in *Proc. 18th IEEE Int. Conf. Image Process.*, Brussels, Belgium, Sep. 2011, pp. 161–164.
10. A. Canclini, L. Baroffio, M. Cesana, A. Redondi, and M. Tagliasacchi, “Comparison of two paradigms for image analysis in visual sensor networks,” in *Proc. 11th ACM Conf. Embedded Netw. Sensor Syst.*, New York, NY, USA, 2013, pp. 62:1–62:2.
11. A. Zabala and X. Pons, “Effects of lossy compression on remote sensing image classification of forest areas,” Int. J. Appl. Earth Observat. Geoinf., vol. 13, no. 1, pp. 43–51, 2011.
12. A. Zabala and X. Pons, “Impact of lossy compression on mapping crop areas from remote sensing,” Int. J. Remote Sens., vol. 34, no. 8, pp. 2796–2813, Apr. 2013.
13. S. Paniga, L. BoAESni, A. Redondi, M. Tagliasacchi, and M. Cesana, “Experimental evaluation of a video streaming system for wireless multimedia sensor networks,” in Proc. 10th IEEE IFIP Ann. Medit. Ad Hoc Netw. Workshop, Favignana Island, Italy, Jun. 2011, pp. 165–170.
14. J. Chao and E. Steinbach, “Preserving SIFT features in JPEG-encoded images,” in Proc. 18th IEEE Int. Conf. Image Process., Brussels, Belgium, Sep. 2011, pp. 301–304.
15. V. ChandAESekhar, G. Takacs, D. Chen, S. S. Tsai, J. Singh, and B. Girod, “Transform coding of image feature descriptors,” in Visual Communications and Image Processing, vol. 7257, M. Rabbani and R. L. Stevenson, Eds. Bellingham, WA, USA: SPIE, 2009, pp. 725–710.