International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

An Improved Discrete Patch Based Reversible Data Hiding for Encoded Color Images

Gayathri.A, Thanga Revathi.S , Christy.S, Pramila.P.V

Abstract: ***This paper proposes a system for encrypting images which is performed by patch wise separable reversible data. In the beginning, with the help of encryption key, a content writer prepares the unique uncompressed image. Then, the data-hider abridge encrypted images with least significant using data smacking key therefore to construct a sparse path that can incorporate with some additional data. The encrypted image data consisting of additional data, will aid the receiver to use only one encryption key to recall both additional data and image after decryption. The proposed system enables the receiver, to bring out the data and retrieving the actual content without an error by using both data-hiding key and encryption keys. The key generated is stored and the log is maintained. Data transmission through public communication system is unsecure due to be inaccuracy and improper exploitation by eavesdropper. The specific problem can be resolved by the technique Steganography, where the hidden messages are written in a way where it is only understood by the sender and intend recipient which gives the complete security for the messages. This proposed method includes Advanced Encryption Standard algorithm for encrypting both the image and the data. In order to achieve efficient working of encryption process, Separable Patch wise Reversible Data Hiding (SPRDH) algorithm is used in rescindable manner. The performance are analyzed using available Classical database images with the metrics Bits per Pixel (BPP). Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE).***

Keywords : Separable Patch-wise Reversible Data Hiding (SPRDH), Reversible data hiding (RDH), Patch Wise Embedding (PWE), Advanced Encryption Standards (AES)

I. INTRODUCTION

One of major tool that is employed for encryption is the cryptography. It acts as a security tool by which the data can encrypted and converted into plain meaningful information from the untidy unknown information / data [1]. The algorithm of Cryptography can be comprehensively classified into symmetric and asymmetric, which are considered as two prominent categories of key algorithms [2]. In symmetric key algorithms, similar key is used to encipher and decipher the evidence from both sender and receiver data. Asymmetric algorithm, commonly known as the Public key algorithm, two separate keys - Private and Public - are used for encryption and decryption [3]. Two different keys are created for every user in the asymmetric method known as the private key and public key. These keys will be used for encryption and decryption process so these keys have to be kept secret from the intruders. Data transmitted over internet using copious dimensions are secretive and trust worthy [4]. Encryption is used to transmit the information accurately and securely. The safeguard envisaged by steganography technique is much better and reliable than what is provided by cryptography. Present days these concepts are widely used due to some common reasons. Cryptography and Steganography are employed in the system with an assertion and assurance that provides the safety and warranty to end uses, towards using the system having its precise functionalities. The process of cryptography helps to guard the data while transmitting till the process of completing the decryption. Steganography provides more protection to the data and helps to hoard enough data along with image. The prime objective of cryptography helps in transforming the data of unintelligible image from the source of third party who is prohibited in accessing the information, wherein the technology of steganography helps in hacking the data from unauthorized individuals with the process of image overlapping the data.

II. LITERATURE SURVEY

Qin.C et al proposed [2015] Separable Reversible Data Hiding in Encrypted Image. In recent years, many researchers have shown interest in signal processing in the encrypted domain because it acts as a very effective and popular path for security [5]. In this process, the original signal is converted into unintelligible data through the means of encryption and so the signal processing is done prior to encryption or post decryption. During certain instances author does not believe service provider processing because of their ability to view the data which is encrypted. During the process of encrypting the transmitted data without having any knowledge the channel provider of the cryptographic key may tend to compress the encrypted data.

W. Li et al proposed [2013] efficient compression of encrypted grayscale images. In the field of cryptography, images transmitted securely plays and eminent role. In order to secure the given data in an unreadable format cryptography is the process enumerated by the author. For discriminating the spatial redundancy in the image a technique called RLC is used which is a lossless compression technique. The comparative study of the lossless data compression algorithm was done and presented the results.

Revised Manuscript Received on February 05, 2020.
* Correspondence Author
Gayathri.A*, Associate Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, SIMATS, Chennai, India
Thanga Revathi.S , Assistant Professor, Department of Information Technology, Rajalakshmi Engineering College, Chennai, India
Christy.S, Assistant Professor, Department of Information Technology, Saveetha School of Engineering, SIMATS, Chennai, India
Pramila.P.V, Associate Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, SIMATS, Chennai, India

In this study, the author used Haar Wavelet compression technique to compress the image with sudden transitions. This technique explains the localization of space frequency to calculate and using of Human Visual System property model. This process of encryption technique restricts only the content owner in retrieving the image.

X. Zhang proposed [2011] Lossy compression and iterative reconstruction for encrypted image. In the last few years we have crossed a vast development in the field of communication technologies which are used in the process of transmitting multimedia information through channels and networks which are highly insecure. This transformation of information through these channels has caused drastic violation of internet privacy policies and also has been a medium to attack personally. The fortification of the image from different kinds of attacks should be done using some safety mechanism. Normally, to protect any data from the intruders, cryptography will be employed but normal data encryption schemes or methods are not applicable for images.

Han-Zhou Wu proposed [2016] a novel technology of Separable Reversible Color Images with the usage of encrypted Palette Images having parameters of partitioning color. RDH methods have been used which depends on lossless compression to create extra space for embedding [6]. Many techniques are introduced later for increasing the embedding capacity which results in making the lowest distortion of images with the application of expansion differentiation, shifting histogram and expansion of error prediction.

Many researchers have attention in Reversible Data Hiding (RDH). In RDH technology, original images are encrypted and the content that are original is reconstructed later embedding the data and so the content owner's privacy remains secured [7]. If the encrypted image contains requisite data in excess, the receiver can decrypt the same based on encryption key, and subsequently obtain the embedded data or vice-versa. Once this process is completed receiver can retrieve the original image bestowing with data-hiding key [8]. This method uses a color partitioning method in order to construct a certain number of embeddable color triples using the palette colors, The experiments are depicted as the method has the capability of extracting data presented and the image recovery is separable and reversible.

III. PROPOSED SYSTEM

This paper introduces Data Hiding using Separable Reversible for encrypted image with Advanced Encryption Standard. The main purpose of cryptography is to change the plaintext to cipher text and the algorithms used are from the advanced Encryption Standard. In order to protect the data, Steganography concept is utilized, with the principle feature of maintaining secrecy of the data so encrypted behind the images. The prime feature of this methodology is – acting as a carrier of data across networks which transmitting data from one user to another. Similar to data hide and encryption key, the sender create the Keys which are similar to them and are auto generated during uploading and transmitting of data across networks over internet. The files are uploaded by the sender only after he logged in to the system securely. Before downloading of the uploaded data, the receiver has to authenticate himself to get authorized for downloading the files with the help of keys provided by the sender via another medium like email, SMS, etc. The original uploaded data cannot be downloaded, if the user fails to authenticate himself with valid keys. The system may misguide the receiver by sending a fake data to the unauthenticated user in the place of the original data. So, adequate security should be provided by the system along with safe transmission of data over internet. For encryption of uploaded data and hiding them behind the image are carried our using Advanced Encryption Standards (AES) algorithm combined with Patch Wise Embedding (PWE) techniques.

AES algorithm helps in providing the best security and helps to faster implementation of both hardware and software. In separable reversible data hiding the receiver side there are three choices. The receiver can use any of the three choices to retrieve the data sent by the sender. If the receiver requires only the image, then it can be retrieved using encryption key. If only the data is required that is fixed into the image, then data hiding key can be used. But if the receiver wants image and data, then the receiver can make use of both the keys. Only because of this, the process is named as Separable Reversible Data Hiding and it is framed in such a way to protect the transmission of data from the intruders. It can be implemented in three steps initially by encrypted image generation, second step by generation of the marked encrypted image, finally data extraction, and image recovery. As initial step the content owner encodes the original image with the help of encryption key to create an encrypted image [9]. Then, the data hider can be a third party owner who can embed data into the image without the knowledge of the content of the image, for example, a database manager or a cloud provider, who are unauthenticated to access the original content. At the receiving side, the content owner are authorized as a third party who can extract the original data either by applying encryption or decryption image [10-12].

3.1 PROPOSED SYSTEM ARCHITECTURE

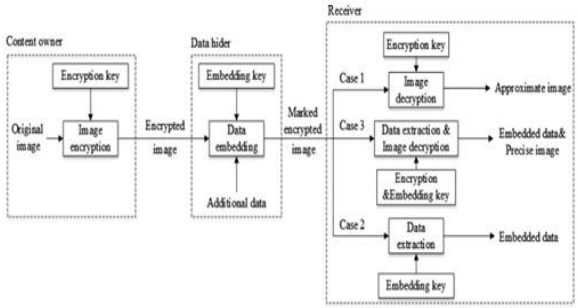


Fig.1: System Architecture

3.2 ADVANCED ENCRYPTION STANDARD

AES algorithm, which is a reiterated using 128 bit block length symmetric key block cipher where the functions on unchanging number of bytes are made unpretentious for application and used for the purpose of data encryption in the system. The algorithm permits similar encryption key as well as decryption key for reducing the difficulties in managing keys.

1) **SubByte** – Each key byte with the aid of S-Box are substituted by converting it with nonlinear invertible S-box, while encoding process, each of the state values are replaced by their subsequent S-Box value, similarly while decryption, every state values altered with equivalent inverse value of S-Box.

2) **ShiftRows**- In shiftrows the latest three rows of regular state are transited and considered as a non-bitwise shift. Left shift bytes is considered to be equivalent to the row number and helpful for the arrangement of state in matrix for applying circular shift to individual row. Later the keys are expanded by preceding the encryption as well as the decryption techniques. The key that are expanded is utilized by add round key step. Due to these advantages, we can ascertain that for encryption of data in a better way, AES algorithm is essential.

3.3 PATCH WISE EMBEDDING

Digital image file uses patch wise bit coding technique for fixing the information. It fixes by pre-placing the binary messages with the patch of sampling points, whereas huge amount of data can be encoded using PWE coding. the diagram below depicts encoding message HEY with 16 bit CD quality PWE technique.

3.3.1 PWE ALGORITHM

The steps involved in performing the encoding using patch level manipulation

Step1: Initially the image files are received as byte form and therefore it is converted to equal or unequal patterns.

Step2: Later the every character of the messages are converted to the equal and unequal pattern.

Step3: Replaces the PWE from image is substituted with PWE bit from character in the message.

ALGORITHIM

The transmission rate of the ideal data in PWE coding ranges as 1kbps/ 1KHz. therefore two sequences of sample bits are replaces using two bit messages. It improves the encrypted data amount which results in increasing of noise in image files, whereas to achieve this the signal contents are decoded earlier deciding the PWE operation, considering the example the noisy stations will be masking the lower bit encoding a sound file recording, where the same noise sounds are audible while playing the sound file containing a piano solo.

The PWD coding technique has the advantage of low complexity in computational algorithm, whereas the disadvantages are the increase in number of PWD coding which is equivalent to the depth of the updated PWD layer are made larger. The second disadvantage is the increase in probability of message detectable and the third disadvantage is about the perceptual transparency of the object is decreased in stenography because of undetectable failure met by stenography.

3.3.2 EXTRACTION ALGORITHM

Step1: Initially three arrays namely Pixel array, Character array and Key array are considered.

Step2: The data in the rear end the image are extracted by decrypting the hidden key.

Step3: later the matches between the actual key and the key array are computed to check error.

Step4: If the hidden key exactly matches with the both decrypted key, then it's authenticated to provide with original data.

Step5: Later the character array is extracted from the data by uploading and downloading operations by the sender and the receiver subsequently.

3.4 DATA EMBEDDING

In the first phase, the owner of the original data encodes the first uncompressed image with the help of encryption key. Due to this function, data-hider will be unknown, regarding the actual data content and sequence of encrypted data bits of the image which are accessed using a data-hiding key. This process is helping to make a sparse space that can fit with application of additional data. Thus the receiver can able to retrieve additional information using data-hiding key, or by obtaining similar images as the original image with the assist of encrypted key.

3.5 IMAGE ENCRYPTION

In this second module, the image with the hidden data is being encrypted and saved in the local disk. In order to decode it a password has to be given manually while those of data being default. The encrypted image is saved in file having extension .png.

3.6 DATA TRANSMISSION, IMAGE RECOVERY AND DATA RECOVERY

The function of data transmission, image and data recovery deals with the process Image Decryption wherein the actual uncompressed image will be encrypted by the original content owner with the help of encryption key. The persistence of the data-hider is to compress the least significant bits in the encrypted image without the knowledge of the original image using data-hiding key. It creates a sparse space for accommodating the additional data. While the receiver will be having both encrypted and decrypted keys, he/she can extract the additional data. This will help in recovering the original content without any error with the application of spatial correlation function in natural images, wherein the quantum of additional data is not too large. This lossless compression technique is used by the embedded data for the encrypted image, the further data will be extracted and thus original content can be also recovered.

Fig. 2: Sample images for Encryption and Decryption

IV. EXPERIMENTAL RESULT ANALYSIS

Experimental analysis is applied to calculate the efficiency of the proposed method. A few sample of images are shown as cover images in order to steganography it and to analyze their behavior. The classical dataset is used for performance valuation. We can calculate the "Peak Signal Noise" ratio between two images using 'The Peak Signal to Noise Ratio' (PSNR) in decibels. For the measurement of quality between original and restored images, this calculation is often used.

The better quality restored or reconstructed image getting through the higher value of the PSNR. For comparison of image quality we can use the error metrics name - 'The Mean Square Error' (MSE) and 'the Peak Signal to Noise Ratio (PSNR)'. For computing the PSNR Value, we need to calculate initially the mean-squared error using the following equation:

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N} \quad (1)$$

Here the value M and the N are considered as the value of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR = 10 \log_{10}\left(\frac{R^2}{MSE}\right) \quad (2)$$

Where, in the input image the maximum fluctuation is denoted as R. In case of the input image is having a double-precision floating-point, then the value for R is considered as 1. However, if the image is having an 8-bit unsigned integer data type, then the value of R is considered as 255.

Table 1 Comparative Analysis of Mean Squared Error for Different Images

IMAGE	Data Embedded Image MSE	Restored Image MSE
Lena	1.1145	0.2145
Baboon	1.9654	0.7554
Pepper	1.4532	0.3321
airplane	1.4353	0.3216
parrot	0.432	0.2315
Ship	1.3216	0.2451

Table 2 : Peak Signal to Noise Ratio Comparative Analysis

IMAGE	Data Embedded Image PSNR(dB)	Restored Image PSNR(dB)
Lena	51.66	57.63
Baboon	48.33	57.72
Pepper	52.67	57.97
airplane	54.23	58.48
parrot	41.68	45.28
Ship	43.56	48.04

Referring to Table 2 – indicates comparative Analysis of Peak Signal to Noise Ratio of data presents in an embedded image and restored image after extraction of data. It also demonstrates that the subject ratio of restored image is much higher than data of embedded image. That means distortion in image will be less. The test image of Lena sized 512X512 pixels is used in the experiment as the original image, and various other images that does not affect the performance of the proposed method.

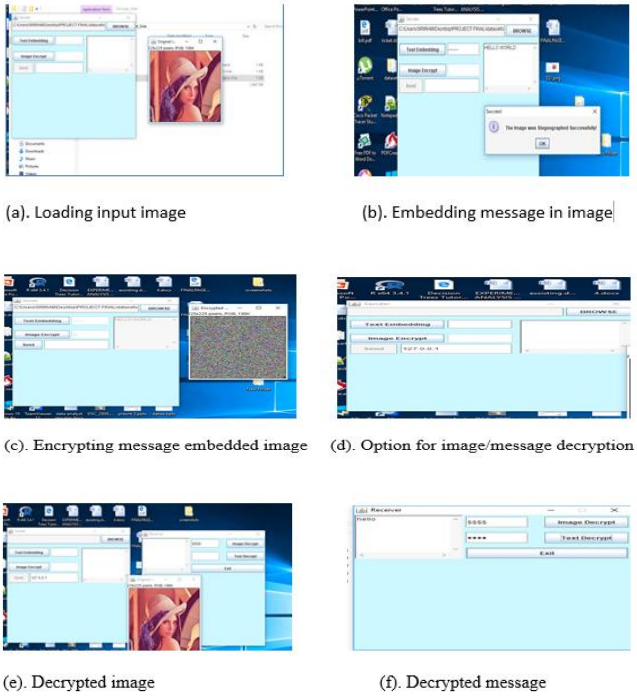
Referring to Table 1 – Embedded rates are listed and directly decrypted Lena image PSNR values are tabulated. For this evaluation, a total of 512X512 = 262,144 bits are hidden in each encrypted unit.

512 x 512 color cover images: (a) Lena, (b) Baboon, (c) Pepper

512 x 512 color cover images: (d) aero-plane, (e) parrot, (f) Ship

Fig. 3: Sample images considered for performance evaluation

As a result, the embedding rate obtained as 1 bit per pixel (bpp), where the similar images are considered as original image, where the original image is completely recovered loosely.



(a). Loading input image (b). Embedding message in image

(c). Encrypting message embedded image (d). Option for image/message decryption

(e). Decrypted image (f). Decrypted message

Fig. 4: Screen shots for Separable Patch wise Reversible Data Hiding

V. CONCLUSION

The prime objective of this system is to afford the end user to have a high security systems for encryption and decryption of image. In the system, the data are encoded in sender's side and subsequently, the same is hidden beneath any of the selected original image. This same data is transferred to the authenticated receiver. Later the receiver receives a secret key in personal e-mail.

The log in of the users are first authenticated by themselves from the system. Later we can obtain the original data back, after authentication by smearing the secret and decryption key. Receivers can obtain the original image only if they can able to apply the secrete key.

REFERENCES

1. Z. Xia, X. Wang, X. Sun, and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340–352, 2016.
2. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2594–2608, 2016.
3. J. Guo, P. Zheng, and J. Huang, "Secure watermarking scheme against watermark attacks in the encrypted domain," Journal of Visual Communication and Image Representation, vol. 30, pp. 125–135, 2015.
4. H. Liu, D. Xiao, R. Zhang, Y. Zhang, and S. Bai, "Robust and hierarchical watermarking of encrypted images based on Compressive Sensing," Signal Processing: Image Communication, vol. 45, pp. 41–51, 2016.
5. C. Qin and X. Zhang, "Effective reversible data hiding in encrypted image with privacy protection for image content," Journal of Visual Communication and Image Representation, vol. 31, pp. 154–164, 2015.
6. Han-Zhou Wu, "Separable Reversible Data Hiding for Encrypted Palette Images With Color Partitioning and Flipping Verification", IEEE Transactions on Circuits and Systems for Video Technology PP(99):1-1 · April 2016.
7. D. Xu and R. Wang, "Context adaptive binary arithmetic coding-based data hiding in partially encrypted H.264/AVC videos," Journal of Electronic Imaging, vol. 24, no. 3, Article ID 033028, 2015.
8. D. Xu and R. Wang, "Two-dimensional reversible data hiding-based approach for intra-frame error concealment in H.264/AVC," Signal Processing: Image Communication, vol. 47, pp. 369–379, 2016.
9. A Gayathri, A Srinivasan , "An efficient algorithm for image denoising using NLM and DBUTM estimation", TENCON 2014-2014 IEEE Region 10 Conference, Page No.1-6, 2014.
10. A Gayathri, A Srinivasan ," Moving object detection by fuzzy aggregation using low rank weightage representation", Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014 pp 335-342.
11. A.Gayathri, S.Christy, "Image de-noising using optimized self similar patch based filter", International Journal of Innovative Technology and Exploring Engineering, 8(12), pp. 1570-157, 2019
12. A.Gayathri, V.Nandhini, "HVS based enhanced medical image fusion", Communications in Computer and Information Science, 250 CCIS, pp. 870-872, 2011.

AUTHORS PROFILE

Dr.A.Gayathri, received the B.E degree in Electronics and Communication Engineering from Periyar Maniammai College of Technology for Women (Bharathidasan University, India) in 2001 and the M.Tech (CSE) degree in Computer Science and Engineering specialization from Bharath University, Chennai, India in 2005. She completed the Doctorate in the Department of Information and Communication Engineering at Anna University. She is currently working as Associate Professor in Saveetha School of Engineering (Department of CSE), SIMATS, Chennai, and Tamil Nadu. She is the member of CSI, IAENG and ACM.

Dr.S.Thanga Revathi is Assistant Professor in Rajalakshmi Engineering College, Chennai.She has completed her Bachelor of Engineering degree in Computer Science and Engineering from Anna University, Chennai with distinction. She has completed her Master of Engineering in Computer Science and Engineering from Bharath University, Chennai. She completed her Ph.D course in Anna University, Chennai and indulged in research work in the field of Data Security in Cloud environment. She has a overall teaching experience of over 13 years in the colleges. She has published papers in referred International and National journals and Conferences.

Dr.S.Christy, is one of the valuable faculty members in Saveetha School of Engineering (Department of IT). She has well over 13 years of teaching experience She has also been awarded Silver Medal in M.Tech. Degree Examination. She has published two subject books for Engineering Students namely "Fundamentals of Computing and C programming" and "Computer Programming", and published 12 Papers in International Journals, out of which two papers are Scopus Indexed. She has the experience of working as software developer for ITC Ltd.

Dr.P.V.Pramila, received the B.E degree in Electronics and Communication Engineering from Bharath Institute of Science and Technology, (Madras University, India) in 2001 and the M.Tech (VLSI) degree in Electronics and Communication Engineering specialization from Satyabama University, Chennai, India in 2008. She completed the Doctorate in the Department of Information and Communication Engineering at Anna University. She is currently working as Associate Professor in Saveetha School of Engineering (Department of CSE), SIMATS, Chennai, and Tamil Nadu.