ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Secure Data Retrieval using Color Histogram

Mohana E [1], Premalatha R [2], Kalaivani M [3]

U.G Student, Department of CSE, Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India[1]

U.G Student, Department of CSE, Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India[2]

Assistant Professor, Department of CSE, Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India[3]

ABSTRACT: There is also an amount of works on data hiding in the encrypted field. Most of the work on Reversible Data hiding focus on the data embedding or extracting on the plain spatial domain. This technique by reserving room prior to encryption with a traditional RDH algorithm, and thus it is simple the data hider to reversibly embed data in the encrypted image. The proposed method can attain real reversibility, that is, data extraction and image revival are free of any fault. Thus the data hider can advantage from the extra space Emptied out in preceding stage to make data hiding process unforced. This scheme can take benefit of all traditional RDH techniques for plain images and attain tremendous performance with no loss of perfect secrecy.

KEYWORDS: Reversible data hiding, Real reversibility, Image Revival.

I. INTRODUCTION

The technique of Reversal data hiding is used to reserve space prior to encryption with a traditional RDH algorithm, and thus it is simple for the data hider to reversibly embed data in the encrypted image.The proposed method can achieve realreversibility, that is, data extraction and image recovery are freeof any error.
The Advanced Encryption Standard(AES) is an encryption for securing susceptible as a likely effect, may ultimately become the effective encryption pattern for commercial transactions in the confidential sector.(Encryption for the US armed and other secret interactions is handled by separate, secret algorithms.)

The algorithm was necessary to be royalty-free for use global and offer security of a adequate level to defend data for the next 20 to 30 years. It was to be simple to execute in hardware and software, as well as in secret environment (for example, in a smart card) and offer fine suspicion against different attack technique. The whole collection procedure was completely open to public scrutiny and remark, it being determined that full visibility would certify the best feasible analysis of the design.

In 1998, the NIST selected 15 candidates for the AES, which were then focus to preliminary analysis by the world cryptographic community, together with the National Security Agency.AES is based on a design standard known as a Substitution permutation network. It is fast in both software and hardware .Unlike its predecessor, DES, AES does not use Feistel Network.AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas, Rijndael can be stated with block and key sizes in any multiple of 32 bits, with a least of 128 bits. The block size has a maximum of 256 bits, but the key size has no theoretic maximum.

AES operates on a 4×4 column-major order matrix of bytes, termed the *state* (versions of Rijndael with a larger block size have additional columns in the state). Most AES controls are done in a distinct finite field. The AES cipher is stated as a number of replications of transformation rounds that change the input plaintext into the final output of cipher text. Every round contains of numerous processing phases, with one that depends on the encryption key. A set of reverse rounds are useful to transform cipher text back into the original plaintext using the similar encryption key.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

II. RELATED WORK

First, the histogram-shifting technique to remedy the two major drawbacks of Tian's algorithm: the lack of capacity control and undesirable distortion at low embedding capacities. We then described two new reversible watermarking algorithms, combining histogram shifting and difference expansion. It is solved using two techniques they are given as follows:

1. The first one using a highly compressible overflow map and the second one using flag bits. A new, reversible, data-embedding technique called prediction-error expansion was then introduced and watermarking algorithms based on the prediction- error expansion technique were presented.
2. This work proposes a novel scheme for separable reversible data hiding in encrypted images. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image.
3. Using a data-hiding key to create a sparse space to accommodate some additional data with an encrypted image containing additional data, if a receiver has the data-hiding key, he can extract the additional data though he does not know the image content.
4. Trust and security have prevented businesses from fully accepting cloud platforms. To protect clouds, providers must first secure virtualized data-center resources, uphold user privacy, and preserve data integrity it is easy for the data hider to reversibly embed data in the encrypted image.
5. Using a trust-overlay network over multiple data centers to implement a reputation system for establishing trust between service providers and data owners. Data coloring and software watermarking techniques protect shared data objects and massively distributed software modules
6.

III.EXISTING SYSTEM

Reversible Data Hiding (RDH) in an encrypted JPEG bit stream. Different existing RDH methods for encrypted spatial-domain images, the proposed technique goals at encrypting a JPEG bit stream into well-ordered structure, and embedding a secret message into the encrypted bit stream by slightly adjusting the JPEG stream. We identify functional bits suitable for data hiding so that the encrypted bit stream carrying secret data can be correctly decoded.

The secret message bits are encoded with error correction codes to achieve a flawless data extraction and image recovery. The encryption and embedding are measured by encryption and embedding keys individually.
If a receiver has both keys, the secret bits can be removed by inspecting the blocking objects of the nearest blocks, and the original bit stream perfectly retrieved. In case the receiver only has the encryption key, he/she can still decode the bit stream to develop the image with enhanced quality without extracting the hidden data.

In the existing System more attention is paid to reversible data hiding (RDH) in encrypted images, then it tolerates the excellent property that the original cover can be lossless and retrieved after embedded data is removed while keeping the image contents privacy.

All previous approaches embed data by reversibly emptying possibility from the encrypted images, which may be subject to some errors on data extraction and/or image. Previous approaches RDH in encrypted images by emptying room after encryption, as opposite to which we proposed by reserving room before encryption. Thus the data hider can profit from the extra space emptied out in preceding stage to make data hiding process unforced.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

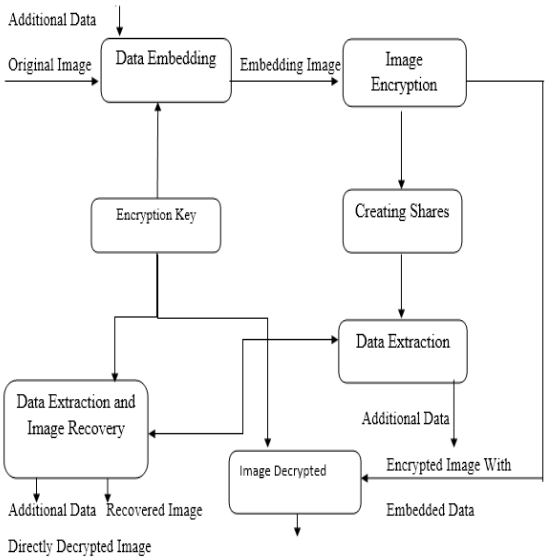


Fig. 1. Sketch of proposed framework

III.PROPOSED SYSTEM

This technique can take benefit of all traditional RDH methods for plain images and attain excellent performance without loss of perfect secrecy. This technique can achieve actual reversibility, distinct data extraction and greatly improvement on the value of marked decrypted images.This processby reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. We can attain real reversibility, that is, data extraction and image retrieval are free of any error.This technique can attain real reversibility, that is, data extraction and image recovery are free of any error.This technique can insert more than 10 times as large payloads for the same image quality as the earlier techniques.

III. REVERSIBLE DATA HIDING

This module includes the login page that contains sender name and password and the receiver name. Then it undergoes reversible data hiding schemes where some schemes are good performance at hiding capacity but have a bad stego image quality, some schemes are good stego image quality.To increase the hiding capacity, multi-layer embedding is used.

IV. IMAGE ENCRYPTION

This module describes about the encryption ofimage that is to be transmitted. Here we use visual cryptography algorithm for encryption of images.So, in first step the image is converted into streams of data array and each data will be encrypted.The shares are created based on the number of users. For example: if 5 users are there,then we create five shares.This algorithm does not use the encryption key because if the key is obtained by some unauthorized users then they will reveal the image very easily.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

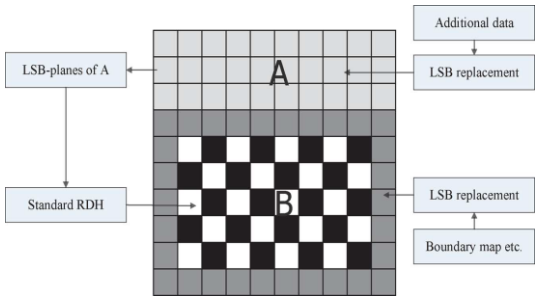


Fig 2. Illustration of image partition and embedding process.

VII.DATA EMBEDDING

This module defines about the embedding the data for secret distribution. It takes one casual encrypted image. Watermark provides the credentials of the provider. Here we use LSB algorithm for data embedding.

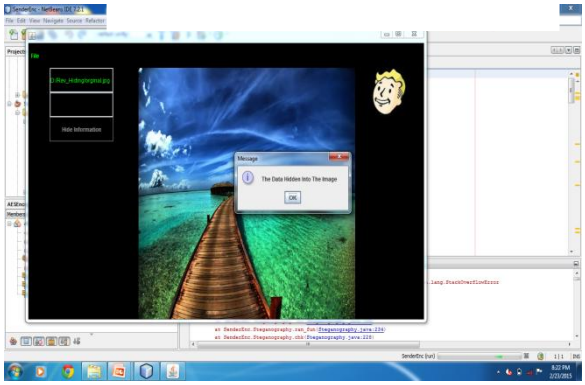


Fig.3.Hidding Data into the image

VIII.DATA PROTECTION

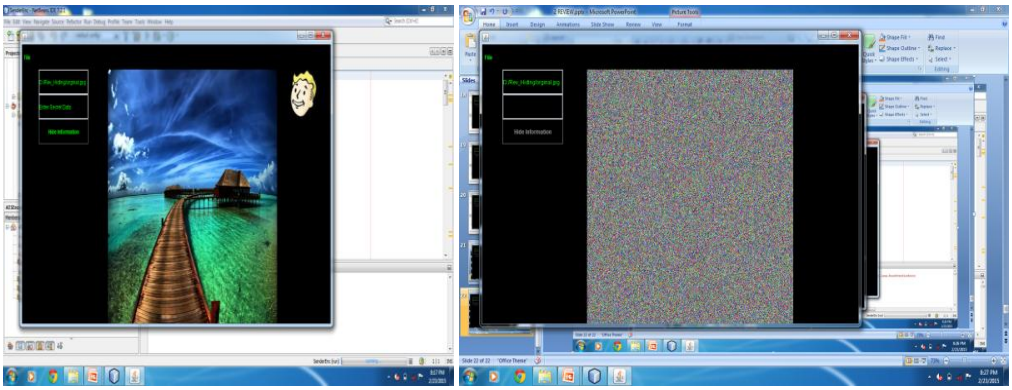
Image recovery is computationally thorough and can profit from offloading to protect energy.To manage the protected data, the image retrieval program may be altered.The altered program must provide satisfactory recovery performance related with the original program and insecure data.In this module ,we can get the clear observation about how the data is being protected in an image that can be retrieved only after following some computational procedures.
The image once protected the data inside then it is encrypted from their original image to avoid intruption of unauthorised users.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015



(a) (b)

Fig. 4. Data Protection.(a) Protected Data(b) Original image and Encrypted Image

VIII.EXTRACTED DATA FROM ENCRYPTED IMAGE

Encrypt Image:The input image is encrypted using a encryption keyprior to the compression of image by which can a image is confidential to view from the illegal user access.Embed Data: In the image the data is embedded later compressing the image by using appropriate technique. The message is insert into the image by means ofdata hiding key.

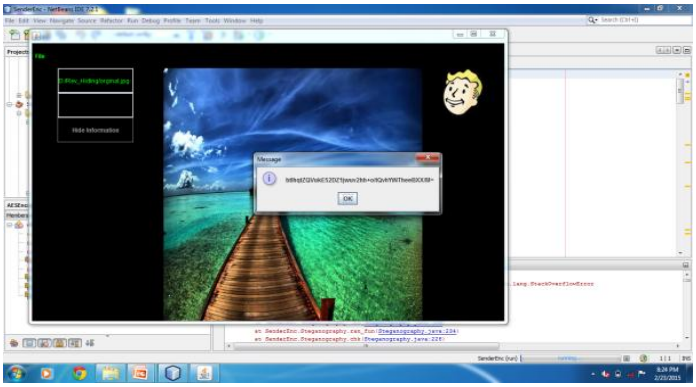


Fig. 5. Extracted data from encrypted image

IX.EXTRACTED DATA FROM DECRYPTED IMAGE

Decrypt Image: The image is decrypted by the encryption key used for encryption of the image. by using the encryption key a user can only access to the image**.De-embed Data:**The data is separated using the data hiding key used for the hiding the data into the image. By using the data hiding a user can access only to the data inside the encrypted image.

Decrypt image and de-embed data: An user who has the both encryption key and data hiding key can access to the image and to the data hidden inside the image both.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

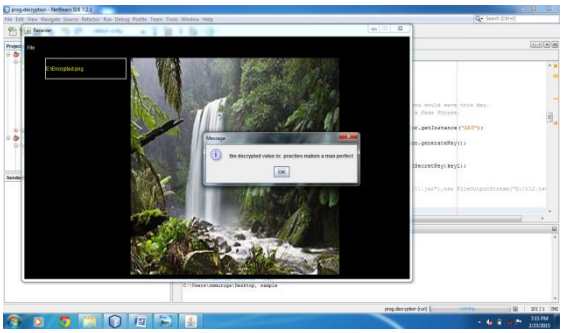


Fig.6 Decrypted image and de-embed data

X.CONCLUSION

Reversible data hiding in encrypted images is a new topic sketch consideration because of the privacy conserving requests from cloud data management. Earlier approaches implement RDH in encrypted images by emptying possibility after encryption, as opposite to which we proposed by means of AES algorithm and LSB methods organized with watermarking. Moreover this novel can have some surplus features for the future work.

REFERENCES

[1] M. Bertalmio, G. Sapiro, V. Caselles, and C. Ballester, "Image inpainting", in Proc. SIGGRAPH, pp. 417–424, 2000.
[2] A. Criminisi, P. Perez, and K. Toyama, "Region filling and object removal by exemplar-based image inpainting.", IEEE Transactions on Image Processing, vol. 13, no.9, pp. 1200–1212, 2004.
[3] Marcelo Bertalmio, Luminita Vese, Guillermo Sapiro, Stanley Osher, "Simultaneous Structure and Texture Image Inpainting", IEEE Transactions On Image Processing, vol. 12, No. 8, 2003.
[4] Yassin M. Y. Hasan and Lina J. Karam, "Morphological Text Extraction from Images", IEEE Transactions On Image Processing, vol. 9, No. 11, 2000
[5] Eftychios A. Pnevmatikakis, Petros Maragos "An Inpainting System For Automatic Image Structure-Texture Restoration With Text Removal", IEEE trans. 978-1-4244-1764, 2008
[6] S.Bhuvaneswari, T.S.Subashini, "Automatic Detection and Inpainting of Text Images", International Journal of Computer Applications (0975 – 8887) Volume 61– No.7, 2013
[7] Aria Pezeshk and Richard L. Tutwiler, "Automatic Feature Extraction and Text Recognition from Scanned Topographic Maps", IEEE Transactions on geosciences and remote sensing, VOL. 49, NO. 12, 2011
[8] Xiaoqing Liu and Jagath Samarabandu, "Multiscale Edge-Based Text Extraction From Complex Images", IEEE Trans., 1424403677, 2006
[9] Nobuo Ezaki, Marius Bulacu Lambert , Schomaker , "Text Detection from Natural Scene Images: Towards a System for Visually Impaired Persons" , Proc. of 17th Int. Conf. on Pattern Recognition (ICPR), IEEE Computer Society, pp. 683-686, vol. II, 2004
[10] Mr. Rajesh H. Davda1, Mr. Noor Mohammed, " Text Detection, Removal and Region Filling Using Image Inpainting", International Journal of Futuristic Science Engineering and Technology, vol. 1 Issue 2, ISSN 2320 – 4486, 2013
[11] Uday Modha, Preeti Dave, " Image Inpainting-Automatic Detection and Removal of Text From Images", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 Vol. 2, Issue 2, 2012
[12] Muthukumar S, Dr.Krishnan .N, Pasupathi.P, Deepa. S, "Analysis of Image Inpainting Techniques with Exemplar, Poisson, Successive Elimination and 8 Pixel Neighborhood Methods", International Journal of Computer Applications (0975 – 8887), Volume 9, No.11, 2010