Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Reversible Cryptography in Encrypted Images by Reserving Room before Encyption

Shailesh Hange, Sagar Divekar, Sandesh Kilanje, Niketan Shinde
Computer Department Pune University
Maharashtra, India

Abstract: Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. In this paper, we propose a novel method by 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. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. Experiments show that this novel method can embed more than 10 times as large payloads for the same image quality as the previous methods.

Keywords: RDH, PSNR, VRAE

I. INTRODUCTION

Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. In this system, we propose a novel method by 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. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error and secure data transfer which can be used in e-banking for transactions.

II. LITERATURE REVIEW

The secret data should stay hidden in a host signal, even if that signal is subjected to manipulations as filtering, resampling, cropping, or lossy data compression. Since no one method is capable of achieving all these goals, a class of processes is needed to span the range of possible applications, Trade-offs exists between the quantity of data and the immunity to modification . In other applications, such as remote sensing and high-energy particle physical experimental investigation, it is also desired that the original cover media can be recovered because of the required high-precision nature. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free, or invertible data hiding techniques. Reversible data hiding facilitates immense possibility of applications to link two sets of data in such a way that the cover media can be losslessly recovered after the hidden data have been extracted out, thus providing an additional avenue of handling two different sets of data[2]. This method of reversible data hiding technique is able to embed about 5–80 kb into a 512x512x8 gray scale image while guaranteeing the PSNR of the marked image versus the original image to be above 48 dB .Many RDH methods have been proposed since it was introduced, Xinpeng Zhang proposed 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 using a data-hiding key to create a sparse space to accommodate some additional data(i.e.,Vacating Room After Encryption (VRAE) method). 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. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data

III. PROPOSED SYSTEM

Purpose:

Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. In this paper, we propose a novel method by 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. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error.

Architecture

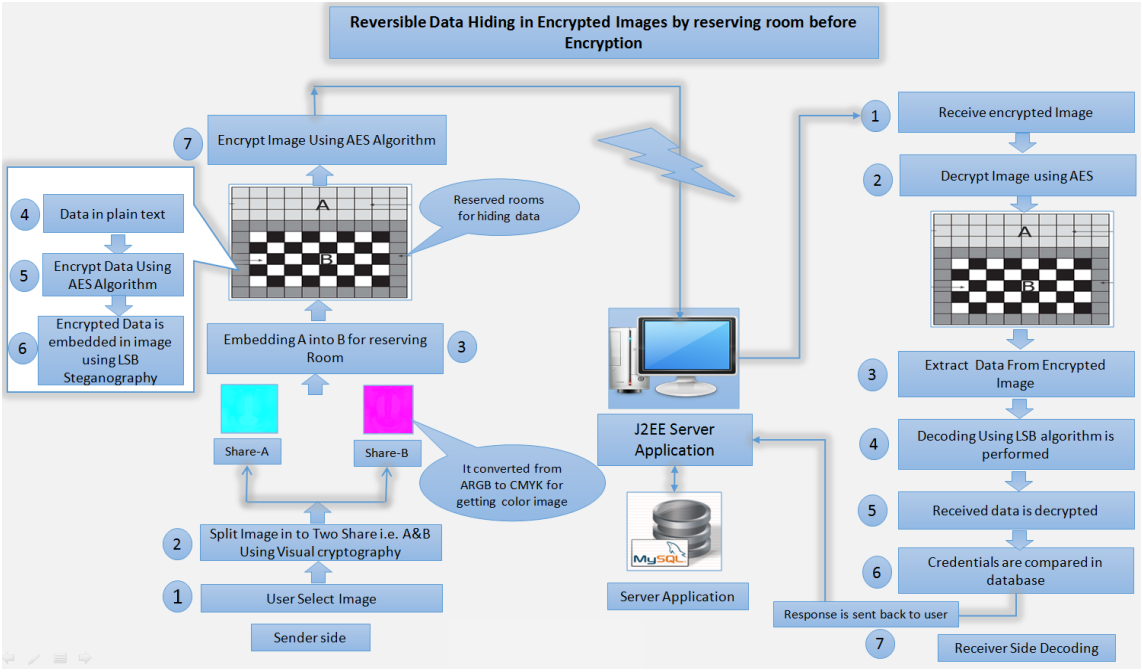

Fig 1:system architecture

Mathematical Model

A mathematical model is a description of a system using mathematical concepts and language. The process of developing a mathematical model is termed mathematical modeling.

Mathematical model consist of three parts:

1. Mapping
2. State Diagram
3. Set theory

➢ Conversion of ARGB to CMYK :-

1. R` = R / 255
2. G` = G /255
3. B` = B / 255

➢ Formulae's of Image Dividation :-

1. k = 1 – max (R`,G`,B`)
2. C = (1 – R` - K) / (1 – K)
3. M = (1 – G` - K) / (1 – K)
4. Y = (1 – B` - K) / (1 – K)

IV. FEASIBILITY STUDY

Feasibility studies aim to objectively and rationally uncover the strengths and weaknesses of the existing business or proposed venture, opportunities and threats as presented by the environment, the resources required to carry through, and ultimately the prospects for success. In its simplest term, the two criteria to judge feasibility are cost required and value to be attained. As such, a well-designed feasibility study should provide a historical background of the business or project, description of the product or service .Feasibility study is conducted after finding out the system's objectives. A feasibility study evaluates the project's potential for success; therefore, the perceived objectivity is an important factor in the credibility to be placed on the study by potential investors and lending institutions. It must therefore be conducted with an objective, unbiased approach to provide information upon which decisions can be based.

V. SYSTEM FEATURES

A. Functional Requirements

- 2.4 GHZ, 80 GB HDD for installation.
- 512 MB memory.
- LAN
- PCs
- Network Cards

B. Non-functional Requirements:

1. Secure access of confidential data (user's details).
2. High Scalability. The solution should be able to accommodate high number of customers and brokers. Both may be geographically distributed
3. Flexible service based architecture will be highly desirable for future extension
4. Better component design to get better performance at peak time

VI. FUTURE SCOPE

The existing system contains some disadvantages so the future scope is to remove the disadvantages by adding reversible manner means, data extraction and recovery of image are free of errors. The PSNR will be improved to get original cover back. In future it may possible that memory space can be reserved before encryption which requires less amount of time for data extraction & image recovery

In future, we will extend this system considering audio, or video files as the cover. In this paper only digital image is considered as cover.

VII. CONCLUSION

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Further more, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.

ACKNOWLEDGMENTS

We are greatly indebted to our college Padmabhooshan Vasantdada Patil Institute Of Technology that has provided a healthy environment to drive us to do this project and thankful to our management for their guidance.

REFERENCES

[1] T. Kalker and F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing(DSP2002), 2002, pp. 71–76.

[2] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding (IH'2011),LNCS 6958, 2011, pp. 255–269, Springer-Verlag.

[3] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans.Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

