International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-1, May 2020

A Reversible High-Capacity Data Hide System Based on Powerful MSB Prediction in Encrypted Images

Raghavendra V, G C Satish

Abstract: ***For encrypted images (RDHEI) reversible data shielding is an important technique for embedding data into the encrypted domain. A hidden key encrypts an original picture, and additional information may be inserted into the encrypted image during or after transmission without knowing the crypting key or the original contents of the picture. The hidden message can be retrieved during the decoding process and the original image can be restored. RDHEI has begun to generate academic attention over the past couple of years. Data privacy has become a real issue with the growth of cloud computing. None of the current methods, however, will allow us to hide a great deal of information reversibly. In this document we propose a new reversible approach with a very high capacity based on MSB (most important bit) forecasting. We present two approaches: a reversible high-capacity data hiding approach with a prediction-correction error (CPEHCRDH) and an integrated-prediction error (EPE-HCRDH) reversible data hiding approach. With this approach, our findings are better than those achieved with the existing state-of-the-art approaches, both in terms of image quality recovered and embedding efficiency.***

Keywords: CPE-HCRDH (high-capacity reversible data hiding with correction of prediction errors).
EPE-HCRDH (high-capacity reversible data hiding with embedded prediction errors).

I. INTRODUCTION

Reversible image data (RDH-EI) is a new technology that has been researched by several researchers and which is derived from reversible data concealed in plaintext photos. This approach is applied by means of a protocol in the cloud storage situation, which involves three individuals, A Cloud server, an image Seller and a licensed customer. The image owner encrypts the content before uploading images to a cloud storage network. The server hides extra messages in encrypted pictures. The RDH-EI protocol ensures the precise retrieval of the secret message by the server. So, without any loss of data, the authorized user can recover the content of the original images.

For labeling of ciphertext in Space of the cloud, RDH-EI is particularly useful. RDH-EI provides first a Stable proprietor encryption algorithm, in order before you upload your photos, when the image owners expect to preserve their privacy. RDH-EI allows the server for hiding data to mark an encrypted image, e.g. by hiding the name, timestamps, and comments in the chipboard text. The labels are then attached in the chip text so that administrators can manage better. Overhead room can also be saved in the meantime. On the other hand, the original content may be recovered losslessly after an approved user downloads the encrypted picture from the cloud. The server generates a metadata file to record information on uploaded images in conventional file management systems. The RDH-EI technology offers a different way to accommodate additional image information on the encrypted bit path. Therefore, for labeling uploaded images no longer needed metadata files.

II. METHODOLOGY

A. Encrypted Domain Image Feature Extraction with SIFT privacy

Privacy has gained significant recognition, but in the multimedia, community is still largely overlooked. Find a cloud computing environment where the computer has plenty of space and can complete tasks. Safe media applications are designed to be handled seriously with privacy protection. Since SIFT has been widely implemented in different fields, this paper is the first to concentrate on the importance of PPSIFT and the security of SIFT functionality extraction and display on the crypted domain and addressing the issue of SIFT protection. Because all operations within SIFT need to be transferred to the encrypted domain, we give the SIFT approach based on homomorphic encryption, in order to protect its privacy. We may prove that PPSI FT is safe against ciphertext only attack and known plaintext attacks by means of security analysis based on the discrete logarithm issue and the RSA. Experimental findings from different case studies show that the SIFT homomorphic encryption-based, privacy-preserving SIFT is close to the original SIFT and that our approach is useful in SIFT applications.

Manuscript received on April 02, 2020.
Revised Manuscript received on April 15, 2020.
Manuscript published on May 30, 2020.
* Correspondence Author
Raghavendra V, School of Computing and Information Technology, REVA University, Bengaluru, Karnataka, India. Email: raghavendravcn@gmail.com
Satish G C, Associate Professor, School of Computing and Information Technology, REVA University, Bengaluru, Karnataka, India. Email: sathish_gc@reva.edu.in

B. Scrambling-based tool for Jpeg image protection

JPEG screwdriving is a versatile device with a GUI and interface which is intuitive and easy to use to protect visual information within a JPEG image (ROI) region of interest. The tool shows a successful integration and use of JPEG image protection tools with an example of a scrolling private privacy filter that allows a wide range of security services such as anonymity, integrity checks, authentication of sources and conditional access.

C. Digital partially linear chaotic maps for dynamic degradation

As chaotic structures of digital computers are implemented with finite precision, their complex characteristics often vary fully from the original models of continuous settings. There appears to be little work in literature on quantitative analysis of such a depletion of digital chaos and how its negative effect on chaos-based digital structures can be minimized. The paper focuses on the 1D piece by pieces linear chaotic maps (PWLCM) and presents some results on a new collection of dynamic indicators that can quantitatively represent the deterioration effects on a fixed-point, finite-precisive digital PWLCM. Therefore, the paper provides a new way to research algorithmically distributed chaos. In addition, the theoretical results achieved by this document would be very useful to consider the negative effect on the actual nature of various digital chaotic systems through dynamic degradation. The proposed dynamic indicators are typical examples of the comparisons of results of various solutions for improving dynamic degradation, the encryption of digital chaotic 1D PWLCM cipher and the architecture of the pseudo-random number generators with desirable characteristics.

D. Enabling Multimedia Database Encrypted Search

Recovery of information is an essential function of retaining confidentiality when a database is maintained on a third-party service provider server. The issue of content-based recovery over encrypted multimedia databases is discussed in this paper. First, the content owner encrypts and then stores indexes and Multimedia Documents on the file. By integrating cryptographic techniques, such as encryption preservation orders and random hash functions, image processing techniques and information recovery, stable index systems have been developed to provide privacy protection and searching functionality that is classified accordingly. Results from a color image encryption database retrieval and a security study of protected indexing schemes under different attack model models show that data confidentiality can be maintained with a high recovery rate. This research has interesting applications in the secure management of multimedia.

III. MODULE DESIGN

Admin Module: Admin will login with admin credentials via the admin login session. The Admin is entitled to install the user profile, delete it and edit it. User accounts and privileges can be handled by admin. Admin can alter your password and your information as well.

Admin module features Include all the admin and user profile information, build user profiles and change password. Based on the project specifications changes, additional functionality may be added to the admin module.

Member/User Module: When the user logs in via the login, the user establishes a self-contained account. The member will encrypt the image with a key during the encryption stage and cover the image data with a special key. The member will decrypt the picture and recover the data information by supplying the secret key in the decryption process.

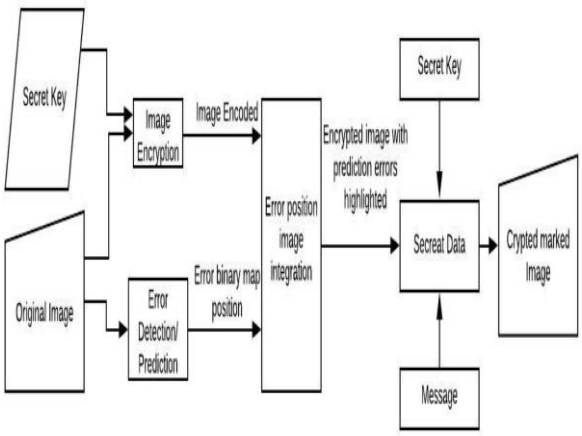
Its key features are self-authentication, user data view, image encryption (images encryption, data hiding, upload and download images), image decryption and secret data retrieval.

IV. BLOCK DIAGRAM

The two solutions we propose: CPEHCRDH (high capacity reversible data with a prediction error correction) and EPE-HCRDH (high capacity reversible data with embedded prediction errors). We recommend two separate solutions. The CPE-HCRDH solution requires the corrections before encryption of prediction errors. The original image is preprocessed to avoid all prediction errors according to the error position map and then the preprocessed image is encrypted. The original image is encrypted directly in the EPE-HCRDH method, but prediction errors are embedded (EPE) after the encryption stage. The MSB of each available pixel will be replaced in an encrypted image with a little of the hidden message during the data hiding time in both approaches. At the end of the cycle, you can extract the embedded data without any errors and recreate your simple picture loss less using the MSB prediction.

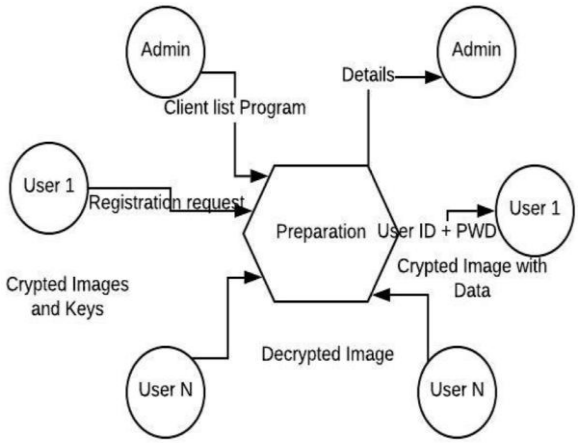
EPE-HCRDH approach

Encoding Phase

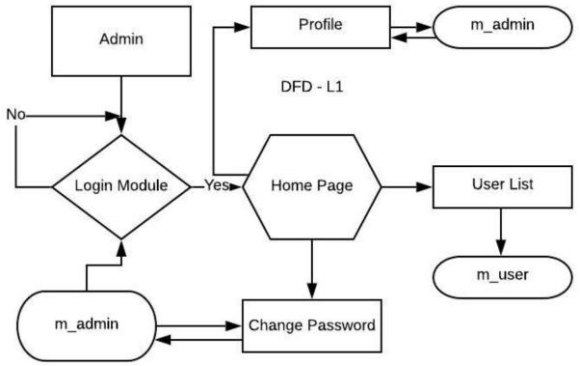


Data Flow of Classification Algorithms

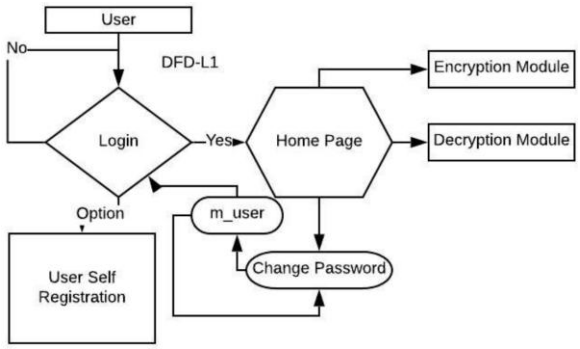
Context Analysis Diagram



Data Flow Diagram of Admin Session



Data Flow Diagram of User Session



V. RESULT AND DISCUSSION

Comparisons with Ciphertext bitstream methods are made with JPEG RDH-EI, and it has been found that the payload is increased by the RDH-EI process. The pressure on both the owner and customer hand is also relieved. The built-in use load is also connected with the JPEG bitstream quality factor. The price factor is therefore increased.

The JPEG image created by the method proposed overcomes the end and improves their Impact visual. The proposed encryption algorithm is also opposed to an intruder. A symbolic JPEG encryption attack examining the original AC Huffman contours in an encrypted bitstream. It also defends against an attack on the algorithm of ciphertext.

VI. CONCLUSION

This paper includes a new RDH-EI protocol. The key goal is to expand the recovery to the comprehensive recovery. The incremental RDH-EI recovery offers better predictive solutions to estimate the original image's LSB layers using three cycles, which outperform state-of-the-art RDH-EI techniques. Given that RDH-EI is equivalent to a rate-distortion problem, both the distortion and the embedding rate should be evaluated. This paper restricts the distortion to three LSB layers for fair comparison and consequently improves the integration efficiency.

REFERENCES

1. P. Bas and T. Furon, "Image database of BOWS-2," http://bows2.eclille.fr/.
2. X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, "High capacity reversible data hiding in encrypted images by patch-level sparse representation," IEEE Transactions on Cybernetics, vol. 46, no. 5, pp. 1132–1143, 2016.
3. T.-H. Chen and K.-H. Tsao, "User-friendly random-grid-based visual secret sharing," IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 11, pp. 1693–1703, 2011.
4. Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," EURASIP Journal on Information Security, vol. 2007, p. 17, 2007
5. X. Gao, L. An, Y. Yuan, D. Tao, and X. Li, "Lossless data embedding using generalized statistical quantity histogram," IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 8, pp. 1061–1070, 2011
6. W. Hong, T.-S. Chen, and H.-Y.Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Processing Letters, vol. 19, no. 4, pp. 199–202, 2012.
7. C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, "Image feature extraction in encrypted domain with privacy-preserving SIFT," IEEE Transactions on Image Processing, vol. 21, no. 11, pp. 4593–4607, 2012

AUTHORS PROFILE

Mr. Raghavendra V. is currently pursuing CSE in M. Tech, at REVA University. He obtained BE in Electronics and Communication degree from VTU, Belgaum. He is working as Manager at Continental Automotive, Bangalore.

Prof. G C Sathish. is an Associate Professor in School of Computing and Information Technology, REVA University, Bengaluru, Karnataka India. He acquired MS degree from BITS, Pilani in 2004. He published twelve articles in reputed International Journals and presented 10 conference papers. He also organized number of workshops, Conferences and Seminars.