Journal of Engineering Sciences
Vol 12, Issue 01, Jan/2021
ISSN NO:0377-9254

RE RANKING MODEL FOR WEB IMAGE USING CLOUD TECHNIQUES

1*Bethala Shirisha, Ph.D scholar, JNTUH, Assistant professor.

Email id: shirishasai34@gmail.com

2*Dr.V. Kamakshi prasad, Professor, JNTUH,

Email id: kamakshiprasad@jntuh.ac.in

Abstract:
Digital image re-ranking algorithms directly retrieve images. Without text messages or images in these algorithms, a semantic gap between the visual feature and high-level semantics of the image exists, which will affect the sequencing performance of retrieval results. In this study, a digital image re-ranking algorithm based on multi-feature fusion was proposed to eliminate the effects of semantic gap on image re-ranking the existing visual reranking methods improve text-based search results by making the use of visual information present in them. These methods are based on low-level visual features, and do not take into account the semantic relationship among images. A main challenge in the research of image re-ranking is that the similarities of visual features do not well associate with semantic meanings of images which infer users search goal. Various reranking methods are developed which are used for image search techniques for different queries. Each method is differentiated with other method and comparative analysis of methods is presented. This paper presents a detail review of different image retrieval and reranking approaches. The purpose of the survey is to provide an overview and analysis of the functionality, advantages, and disadvantages of the existing image reranking methods, which can be useful for researchers

1.0 INTRODUCTION

Reversible data hiding (RDH) in images is a method, by which the original cover can be listlessly recovered after the embedded message is extracted. This technique is widely used in medical images, military imagery and law forensics, where no less quality of the original cover is allowed. Since the first introduced, RDH method has attracted considerable research interest. In the theoretical part, Kalker and Willems established a rate-distortion method of RDH, through which they proved the rate-distortion bounds of RDH for memory-less covers and proposed a recursive code construction which, however it does not approach the bound. Zhang et al. was improved the recursive code construction for binary covers and proved that this construction can achieve the rate distortion bound as long as the compression algorithm reaches the entropy, that establishes the equivalence between the both data compression and RDH for binary covers.

In practical aspect, a lot of RDH techniques have emerged in recently. Fridrichet al. constructed a general framework for RDH. In this first extracting compressible features of original cover and then compressing them lossless and spare space can be saved for embedding auxiliary data. A most popular method is based on difference expansion (DE), in which the difference of each pixel group is expanded, e.g., is multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another hopeful strategy for RDH is histogram shift (HS), in which space is saved for data embedding by shifting the bins of histogram of grey values. The state-of-art methods usually combined the both DE and HS to residuals of the image, e.g., the expected errors, to achieve better performance.

With regard to providing confidentiality for images, encryption is an effective and popular means as it converts the original and meaningful content to incomprehensible one. Al-though few RDH techniques in encrypted images have been published yet, we have some promising applications if RDH can be applied to encrypted images. In Hwang et al. advocated a reputation-based trust-management scheme enhanced with data coloring (a way of embedding data into covers) and software watermarking, in that data encryption and coloring offer possibilities for upholding the content owner's privacy and data integrity. The cloud service provider has no right to introduce permanent distortion during data coloring into encrypted data.

Hence, a reversible data coloring technique based on encrypted data is preferred. Suppose a medical image database is stored in a data centre, and a server in the data centre can embed notations into an encrypted version of a medical image through a RDH technique. With this, the server can manage the image or verify its integrity without having the knowledge of the original content, with that he patient's privacy is protected. On the further hand, a doctor is having the cryptographic key can be decrypt and restore the image in a reversible manner for the purpose of further diagnosing. Some efforts on RDH in encrypted images have been made. Zhang divided the encrypted image into several blocks by flipping the 3 LSBs of the half of pixels in each block and room can be vacated for the embedded bit.

With that the data extraction and image recovery proceed by finding which part has been flipped in one block. This method can be realized with the help of spatial correlation in decrypted image. In Hong et al. ameliorated Zhang's method at the decoder side by further exploiting the spatial correlation using a different approximation equation and side match technique to achieve much lower error rate. These two methods are mentioned above rely on spatial correlation of original image to extract data. It remains the encrypted image should be decrypted first before data extraction. To separate the data extraction from image decryption for data embedding following the idea of compressing encrypted images.

The compression of encrypted data can be formulated as source coding with side information at the decoder, with that the typical method is to generate the compressed data in lossless manner by exploiting the patterns of parity- check matrix of channel codes. In the method compressed the encrypted LSBs to vacate room for additional data by finding syndromes of a parity -check matrix and the side information used at the receiver side is also the spatial correlation of decrypted images. In all the three methods try to vacate room from the encrypted images directly.

2.0 LITERATURE REVIEW

Piva, A., Bianchi, T. and De Rosa, A., (2010) Recently, with the development of cloud computing, more and more secret data are stored in cloud. Reversible data hiding in encrypted images is a technique that makes contribution to cloud data management in privacy preserving and data security. In previous works, Zhang and Hong presented two reversible dada hiding methods in encrypted images, respectively. However, Zhang's work neglected the pixels in the borders of image blocks, and Hong et al.'s research only considered two adjacent pixels of each pixel. In addition, their works only considered that all image blocks are embedded into additional data. In this paper, we propose a novel method of evaluating the complexity of image blocks, which considers multiple neighboring pixels according to the locations of different pixels. Furthermore, data embedding ratio is considered. Experiments show that this novel method can reduce average extracted-bit error rate when the block size is appropriate.

Rial, A., Deng, M., Bianchi, T., Piva, A. and Preneel, B., (2010) A novel reversible data hiding technique in encrypted images is presented in this paper. Instead of embedding data in encrypted

images directly, some pixels are estimated before encryption so that additional data can be embedded in the estimating errors. A benchmark encryption algorithm (e.g. AES) is applied to the rest pixels of the image and a special encryption scheme is designed to encrypt the estimating errors. Without the encryption key, one cannot get access to the original image. However, provided with the data hiding key only, he can embed in or extract from the encrypted image additional data without knowledge about the original image. Moreover, the data extraction and image recovery are free of errors for all images. Experiments demonstrate the feasibility and efficiency of the proposed method, especially in aspect of embedding rate versus Peak Signal-to-Noise Ratio (PSNR).

Chen, B. and Wornell, G.W., (2001) In this paper, a novel reversible data hiding (RDH) scheme for encrypted digital images using integer wavelet transform, histogram shifting and orthogonal decomposition is presented. This scheme takes advantage of the Laplacian-like distribution of integer wavelet high-frequency coefficients in high frequency sub-bands and the independence of orthogonal coefficients to facilitate data hiding operation in encrypted domain, and to keep the reversibility. Experimental results has demonstrated that this scheme outperforms all of other existing RDH schemes in encrypted domain in terms of higher PSNR at the same amount of payload. Compared with the state-of-the-arts, the proposed scheme can be applied to all natural images with higher embedding rate.

Cheng, B., Zhuo, L., Bai, Y., Peng, Y. and Zhang, J., (2014) Digital image sometimes needs to be stored and processed in an encrypted format to maintain security and privacy, e.g., cloud storage and cloud computing. For the purpose of content notation and/or tampering detection, the cloud servers need to embed some additional information directly in these encrypted images. As an emerging technology, reversible data hiding in the encrypted domain will be useful in cloud computing due to its ability to preserve the confidentiality. In this paper, a novel separable and error-free reversible data hiding scheme in encrypted images is proposed. After analyzing the property of interpolation technology, a stream cipher is utilized to encrypt sample pixels and a specific encryption mode is designed to encrypt interpolation-error of non-sample pixels.

Manjunath, B.S., Ohm, J.R., Vasudevan, V.V. and Yamada, A., (2001) In this paper, we propose a novel reversible data hiding scheme in encrypted image. The content owner encrypts the original image with the encryption key to achieve privacy protection for image content, and then, each block of the encrypted image is embedded with one secret bit by the data hider using the data-hiding key. Through the elaborate selection for partial pixels to be flipped, data hiding process only conducts slighter modifications to each block, which leads to significant improvement of visual quality for the decrypted image. The receiver can easily decrypt the marked, encrypted image using the encryption key, and then, through the data-hiding key and an adaptive evaluation function of smoothness characteristic along the isophote direction, secret data can be extracted from the decrypted image, and the original image can further be recovered successfully. Experimental results demonstrate the effectiveness of the proposed scheme.

3.0 RESEARCH METHODOLOGY

Since losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient, so it is obsessed to find novel RDH techniques working directly for encrypted images. In this RDH technique if we reverse the order of encryption and vacating room, which is reserving room prior to image encryption at content owner side “reserving room before encryption (RRBE)”is framework used when the RDH tasks in encrypted images would be more natural and much easier. Then, the data embedding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous

emptied out. In which data extraction and image recovery are identical to that of Framework VRAE.

Particularly, standard RDH algorithms are the ideal operator for reserving room be-fore encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. Because in this new framework, the customary idea that first losslessly compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy. Next, we elaborate a practical method based on the Framework "RRBE", which primarily consists of four stages: 1) generation of encrypted image, 2) data hiding in encrypted image, 3) data extraction and 4) image recovery. Here, the reserving operation we adopt in the proposed method is a traditional RDH approach.

Technologies used

- Shamir's Secret Sharing (SSS) Scheme
- Histogram Modification: A reversible data hiding scheme (2) worked on histogram modification. The principle behind the histogram modification process based on the neighbor pixel differences instead of the host image's histogram.

Software's used

- MATLAB

4.0 RESULTS

In this scenario, the communication overhead of the proposed scheme is less than that of RCE by about 300-byte with the same level of ownership management capability8 . Next, we analyze and measure the computation cost incurred when a data owner encrypts and decrypts data during upload and download phases, respectively. The computation cost is shown in Table 3 in terms of the computation of a cryptographic hash function for key generation, tag generation (the hash function is also used for key encryption/decryption in LR [19]), data encryption/decryption, and key decryption. The comparatively negligible bitwise exclusive-or operations are ignored in the computation analysis results. For each operation, we include a benchmark timing. Each cryptographic operation was implemented using the Crypto++ library ver. 5.6.2 [34] on a 3.4 GHZ processor PC. The key parameters were selected to provide a 128-bit security level. The implementation uses an MD5 as a cryptographic hash function to generate a 128-bit key and tag, and an AES with Electronic Code Book (ECB) mode as an encryption/decryption function.

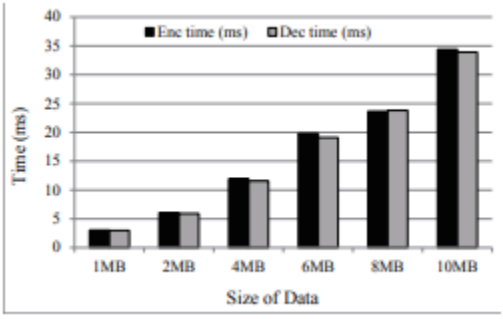

Figure 4.1: Encryption and decryption time

Data encryption and decryption time, denoted by Enc and Dec, respectively, in Table, are measured for different data sizes as shown in Fig, which increase in proportion to the size of data. On the basis of the encryption and decryption time, we measured the total computation cost for the upload and download of each scheme, as shown in Fig., respectively. For the upload

procedure, the proposed scheme requires the same computations as the CE and RCE schemes. For the download procedure, the proposed scheme needs one more key decryption operation than does the basic RCE scheme.

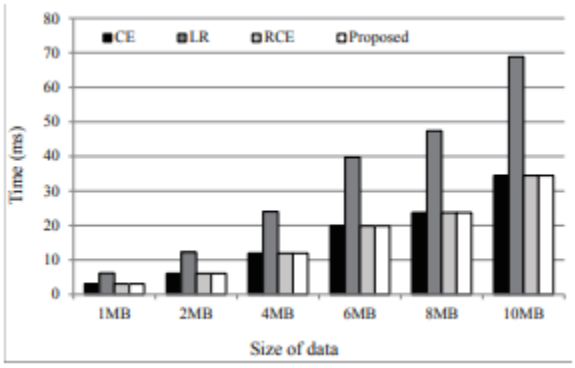

Figure 4.2: Computation time for upload

However, since the symmetric key size is much smaller than the typical data size in the cloud (e.g., document file, or multimedia data), the additional 128-bit key decryption time (i.e., 0.129 ms) in the proposed scheme would be relatively negligible as compared to the data decryption time in a pragmatic cloud computing system as depicted in Fig. The measured computation time for upload and download is described. More experimental results with diverse file size (100KB ~ 1000MB) can be found in the supplementary file.

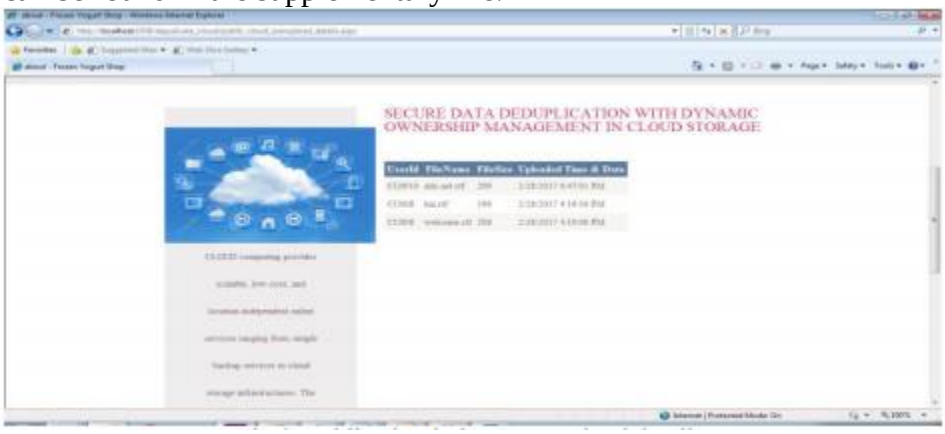

Figure 4.3: public cloud view user upload details

Where the public cloud view user details which gives who viewed the uploaded file and public cloud view user upload details give details of users who uploaded files into public cloud.

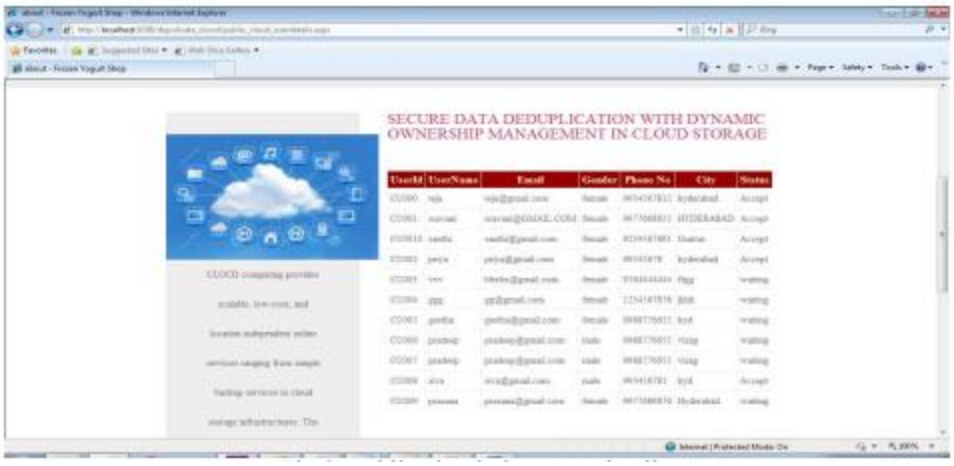

Figure 4.4 : public cloud view user details

To evaluate the effect of number of stored files in the system, we upload 10,000 10 MB unique files to the system and record the breakdown for every file upload. Token checking is done with a hash table and a linear search would be carried out in case of collision.

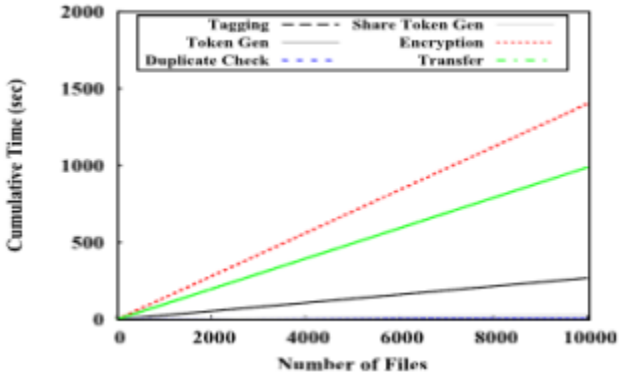

Figure 4.5 : Time breakdown for different number of stored files

To evaluate the effect of privilege set size, we upload 100 10 MB unique files with different size of the data owner and target share privilege set size. While the number of keys increases 100 times from 1,000 to 100,000, the total time spent only increases to 3.81 times and it is noted that the file size of the experiment is set at a small level (10 MB), the effect would become less significant in case of larger files.

CONCLUSION:

Digital images with similar visual feature may not have similar semantic contents. To eliminate the effects of the semantic gap between background visual feature and high-level semantic attributes in digital images on image reranking, a digital image re-ranking algorithm based on multi-feature fusion is proposed by using Holiday, Oxford, and Paris as database samples. The proposed algorithm is used to explore the retrieval intention of the users and correct the effects of semantic gap on the relevance fraction of digital images. The conclusions drawn are as follows Image search Reranking method is used to refine text-based image search by its visual content. It is used mainly to get a refined image search as per the fulfillment of the user. Here, various image retrieval methods and the reranking methods which are proposed by earlier researchers for the better development in the web image search are discussed along with their advantages and disadvantages. These methods are categorized in different reranking strategies depending on the used approaches such as clustering based reranking, classification based reranking and graph

based reranking However, the proposed algorithm has poor recognition accuracy to the semantic attributes of digital images. Another appropriate way to express the semantic attributes of digital images should be investigated.

BIBLIOGRAPHY

[1] Piva, A., Bianchi, T. and De Rosa, A., 2010. Secure client-side ST-DM watermark embedding. IEEE Transactions on Information Forensics and Security, 5(1), pp.13-26.

[2] Rial, A., Deng, M., Bianchi, T., Piva, A. and Preneel, B., 2010. A provably secure anonymous buyer– seller water marking protocol. IEEE Transactions on Information Forensics and Security, 5(4), pp.920-931.

[3] Chen, B. and Wornell, G.W., 2001. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. IEEE Transactions on Information Theory, 47(4), pp.1423- 1443.

[4] Cheng, B., Zhuo, L., Bai, Y., Peng, Y. and Zhang, J., 2014, December. Secure index construction for privacy-preserving large-scale image retrieval. In Big Data and Cloud Computing (BdCloud), 2014 IEEE Fourth International Conference on (pp. 116-120). IEEE.

[5] Manjunath, B.S., Ohm, J.R., Vasudevan, V.V. and Yamada, A., 2001. Color and texture descriptors. IEEE Transactions on circuits and systems for video technology, 11(6), pp.703-715.

[6] Wang, C., Cao, N., Ren, K. and Lou, W., 2012.Enabling secure and efficient ranked keyword search over outsourced cloud data. IEEE Transactions on parallel and distributed systems, 23(8), pp.1467-1479.

[7] Hsu, C.Y., Lu, C.S. and Pei, S.C., 2012. Image feature extraction in encrypted domain with privacypreserving SIFT. IEEE Transactions on Image Processing, 21(11), pp.4593-4607

[8] Lu, C.S. and Liao, H.Y., 2001. Multipurpose watermarking for image authentication and protection. IEEE transactions on image processing, 10(10), pp.1579-1592.

[9] Lu, C.S., Huang, S.K., Sze, C.J. and Liao, H.Y.M., 2000. Cocktail watermarking for digital image protection. IEEE Transactions on Multimedia, 2(4), pp.209-224.

[10] Lu, C.S. and Liao, H.Y., 2003. Structural digital signature for image authentication: an incidental distortion resistant scheme. IEEE Transactions on Multimedia, 5(2), pp.161-173.

[11] Lin, C.Y. and Chang, S.F., 2001. A robust image authentication method distinguishing JPEG compression from malicious manipulation. IEEE Transactions on Circuits and Systems for Video Technology, 11(2), pp.153-168.

[12] Lin, C.Y., Wu, M., Bloom, J.A., Cox, I.J., Miller, M.L. and Lui, Y.M., 2001.Rotation, scale, and translation resilient watermarking for images. IEEE Transactions on image processing, 10(5), pp.767-782.

[13] Fuh, C.S., Cho, S.W. and Essig, K., 2000. Hierarchical color image region segmentation for content-based image retrieval system. IEEE Transactions on Image Processing, 9(1), pp.156-162.

[14] Lai, C.C. and Chen, Y.C., 2011. A user-oriented image retrieval system based on interactive genetic algorithm. IEEE transactions on instrumentation and measurement, 60(10), pp.3318-3325.

[15] Mukherjee, D., Chae, J.J. and Mitra, S.K., 2000. A source and channel-coding framework for vector-based data hiding in video. IEEE Transactions on Circuits and Systems for video technology, 10(4), pp.630-645.

[16] Tiakas, E., Rafailidis, D., Dimou, A. and Daras, P., 2013. MSIDX: multi-sort indexing for efficient content-based image search and retrieval. IEEE Transactions on Multimedia, 15(6), pp.1415-1430.

[17] Khelifi, F. and Jiang, J., 2010. Perceptual image hashing based on virtual watermark detection. IEEE Transactions on Image Processing, 19(4), pp.981-994.
[18] Cannons, J. and Moulin, P., 2004. Design and statistical analysis of a hash-aided image watermarking system. IEEE Transactions on Image Processing, 13(10), pp.1393-1408.
[19] He, J., Li, M., Zhang, H.J., Tong, H. and Zhang, C., 2006. Generalized manifold-ranking-based image retrieval. IEEE Transactions on image processing, 15(10), pp.3170-3177
[20] Shashank, J., Kowshik, P., Srinathan, K. and Jawahar, C.V., 2008, June. Private content based image retrieval. In Computer Vision and Pattern Recognition, 2008.CVPR 2008. IEEE Conference on (pp. 1-8). IEEE.