Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 9, September -2017

Double Faced Data Hiding in Images and Videos using RIT Approach

[1]Santosh Dinkar Kale, [2]Dr. Neeta Deshpande

[1,2] *D. Y. Patil College of Engineering, Akurdi, Pune*

Abstract—*Cloud is an efficient way to outsourced data and gets relief from heavy management of data. It is vital that with the management of data to enable privacy of cloud server. For such privacy and data management scenario, reversible data hiding in encrypted images (RDH-EI) appeal to more and more researcher's attention. We have proposed RDH-EI approach. It is based on reversible image transformation (RIT). In proposed approach, original image content is transformed to the content of target image which is equalized in size. The target image is used to encrypt the content of original image and then outsourced to cloud server. Using RDH methods cloud server can easily embed original image into "encrypted image". Therefore, data embedding process at user-side can efficiently executed. Proposed system satisfies image quality needs and large embedding capacity. Along with image reversible hiding proposed system contributes RDH video encryption and decryption.*

Keywords: *— reversible data hiding, image encryption, reversible image transformation, privacy protection, outsourced storage in cloud*

I. INTRODUCTION

Cloud storage is an internet based computing which gives many services at very cheap cost. Large number of users as well as big firms outsourced their data to cloud to reduce heavy burden of data management. To store multimedia files such as, images, audios & videos required more space than textual documents. To provide more security for data, data owner embed contents into image and then outsourced it to cloud server. Therefore, cloud server cannot distort data from embed images. To utilize such image embedding, RDH technology is required, using which original images can losslessly found after the embedded message is extracted. It is mainly used in medical imagery, military imagery, law forensics and the area in which no distortion of the original cover is allowed. Previously there are several RDH methods on images have been proposed which viewed as a process of semantic lossless compression. In this some space is saved for embedding extra data by losslessly compressing the image. In semantic compression approach original and compressed images are closed to each other. Therefore, PE i.e. Prediction error has small entropy and they are easily compressed. Using this approach, one can get marked images with good visual quality. RDH methods generates PE's as the sequence of host and message is reversible embed to host sequence by converting its histogram with the methods like, histogram shifting (HS) or difference expansion (DE). Optimal histogram modification algorithm is proposed by Zhang et al. for estimating the optimal modification probability.

It is challenging task to protect privacy of image content in cloud environment. Just while ago, many private photos of Hollywood actress leaked from iCloud. Even if RDH is efficient to manage outsourced images, it cannot protect content of image. The basic approach to provide privacy for data is "encryption". Therefore we proposed RDH-EI i.e. RDH in encrypted images approach. In this data is reversibly embedded into the image but cannot get any knowledge about the image contents. It is proposed by inspiring the problems of data privacy. RDH is belonging to two frameworks such as, RRBE i.e. reserving room before encryption" and VRAE i.e. vacant room after encryption. In RRBE, RDH method is used by image owner to unfilled plain images. Then encryption is performed over an image and then uploaded to cloud. Cloud can easily embed data into reserve rooms of encrypted image whereas, in VRAE, data compression is formulated as source coding. For decompression of data side information decoder is used. In both approaches, ciphertetext-formed images are outsourced to cloud server. But ciphertexts with some careless encryption may crack by cloud as it always curious to gather information from outsourced files. And curious cloud is more attracted towards encrypted images hence privacy is an essential need of outsourced images. The proposed RDH-EI is based on RIT which transfers the contents of original image into semantic image; it is known as, "reversibility". Also it can loselessely restored from transformed image. "Semantic Transfer Encryption (STE)" is transformed image which also in encrypted format. In proposed RIT, cloud server can easily embeds the data in encrypted image. RDH-EI is user free scenario for public cloud. In this public cloud ask users how to encrypt and decrypt their data.

II. RELATED WORK

A reliable surface network over multiple data centers is implemented to establish trust between service providers and data owner. Cloud trust is social problem. The proposed technology gives trust, justice, reputation, credibility, and assurance in network applications. Data integrity issues are addressed in this paper. A reputation-based trust-management scheme is introduced with data coloring and software watermarking. For secured infrastructure as a service author stated an example of Amazon's Elastic Compute Cloud. Data coloring approach disconnects the user access and isolates sensitive

information from provider access. This approach protects the data objects from getting damaged, stolen or deleted. Also watermark based schemes acquires less overheads in the coloring as well as de-coloring process [1].
Two tailored reversible watermarking techniques for the clinical atlas by splitting their inherent characteristic is explained in [2]. First technique is designed for atlases with homochromous framework which achieves the reversibility. Another technique is applied to any atlas in palette format, and inquires zero misuse to the watermarked atlas by simply modifying the palette. Security issues to digital medical data which categorized into three aspects such as, confidentiality, availability and authentication. [2].
S. Asoodeh, et al discussed challenges of two dimensional source code encryption with specified index. A general converse result for number of information is provided by them. To compress private as well as public sources with secured source coding problem in which encoder must compressed the source code into specified index. Dealing with the problem of two-dimensional source code encryption they gives more and more basic utility equivocation tradeoff. But in this paper, there is problem with moment that the bounds are tight in general. Furthermore, they were planning for developing schemes for general cases [3].Reversible data hiding scheme consists of two phases such as; in the first phase host sequence is constructed with the accurate histogram through prediction errors. In second phase they were focused on method of histogram modification for RDH. In this phase they utilized compression and decompression processes. Equivalency between loseless data compression and RDH is generated. The proposed approach is useful in medical imaginary, military imaginary etc it covers the precious as well as damaged images. It is quite helpful in the video error-dissimulation coding. In this paper they proposed code construction for memory-less hosts [4]. V. Sachnev et al[5] proposed reversible and loseless watermarking algorithm without using location information. For comparison of proposed reversible watermarking scheme different images are used and compared with the other four methods. It reduces the size of location map key goals are achieved. Location maps include flags having value either 0 or 1 [6]. Location maps are huge in size; if they are compressed they may occupy part of payload. The proposed approach moderately increases the capacity and it also required additional information. It exploits the prediction errors with less variance so that better improvements can achieve. Local prediction in various expansions of reversible watermarking in discussed in [6]. Least square predictor is evaluated on square block pixel center. The proposed local predictor applies the predictor order and it is more general. The substitution should be applied on LSB to neglect artifacts where the compression ratio is low. There are four contexts namely, rhombus context and the ones of MED, GAP and SGAP predictors for which reversible watermarking was analyzed. The proposed approach outperformed the global least square and fixed prediction based counterparts and presets the best results.
RCC i.e. recursive code construction approach is represented by W. Zhang, X. Hu, et al and N. Yu, et al[7]. It is developed for rate distortion bound of RDH. OTPM method i.e. optimal transition probability matrix is proposed for specific distortion metrics. It calculates rate distortion bound of RDH for general cases. Properties of OTPM methods are needed to evaluate capacity for RDH in the process of encoding and decoding. RCC reduces the embedding distortion of RDH. In RDH, it firstly solves the problem of optimization. Hamming distance is useful in RDH for other distortion metrics [8]. A unified algorithm estimates the optimal transition probability matrix for generalized distortion metrics. A fast algorithm is also introduced in [8]. It resolves optimal marked-signal distribution. As we know familiar with RDH which is reversible data hiding technique basically used to hide the information with their characteristic. It is further extracted and covers itself. In DE i.e. different expansion approach differences of each pixel groups are expanded. The proposed algorithm estimates the optimal marginal distribution which is faster than the BFI algorithm. A novel reversible image data hiding method (RIDH) is proposed in [9]. Two class SVM classifier is demonstrated to separate encrypted and non-encrypted patches of images, it gives higher embedding capacity and it also able to reconstruct original image and embedded message. Mainly, RIDH algorithm is designed for plaintext documents. In this message bits are embedded into the original image hence we can say that it works for lossless compression algorithm for compression certain features of images. The DE i.e. different expansion method improves the prediction error expansion (PEE)-based strategies which offers the state-of-the-art capacity distortion performance. The proposed two-class SVM classifier can efficiently separate outs the encrypted and non-encrypted patches of image. A separable reversible data hiding in encrypted images is discussed in [10]. RDH method in encrypted images using distributed source coding is defined in [11]. A LDPC is low density parity check codes used to select bit series Slepian-Wolf encoded. A separable reversible data hiding method is used for encrypted images. With the help of embedding keys and the original image can be perfectly recovered with high embedding payloads and good quality of image reconstruction. It neglects the operations of room-reserving by the sender. In this paper, experimental results shows that the previous methods such as, VRAE method, DSC substantially increases the payload. Encryption and embedding keys are used to protect embedding and recovery an adversary is unable to break into the system without these keys [11].Reversible data hiding technique in encrypted images embedding data pixels are estimated before encryption and AES algorithm is applied to the other pixels of images. To improve performance of reversing the order of encryption and vacating room is introduced in [12]. A better correlation between neighbor pixels by considering the patch-level sparse representation when hiding the secret data explored in [13]. RDH method aims to recover both the embedded secret information and the original cover image. A high capacity separable reversible data hiding in encrypted images (HC_SRDHEI) is introduced for better exploit the correlations of neighbor pixels. A patch-based RDHEI scheme defined correlation of pixels within the patch. It performed significantly better than the traditional RDHEI methods. RDHEI scheme is mainly divided into two categories namely, VRAE and RRBE. The proposed method HC_SRDHEI works for three aspects such as, generation of encrypted image, hiding data into encrypted image and extraction of data and recovery of image.

III. PROBLEM STATEMENT

"To design and develop a system to hide data into images using RIT based RDH-EI approach."

IV. PROPOSED SYSTEM

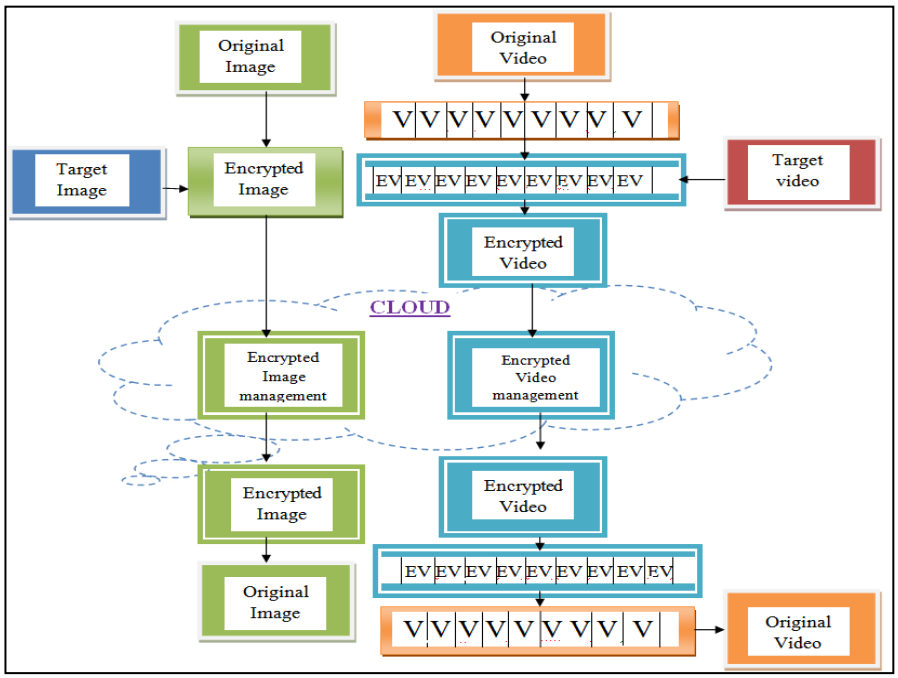

Figure 1: System architecture

1. For Image RDH[image uploading]:
1. Select original image
2. Select target image
3. Check for equisized
4. Encrypt data using AES
5. Embed data into image using RDH
6. Upload encrypted image on cloud

2. To download image:
1. Get target image
2. Anti transformation
3. Download original image
4. Get data

3. For Video RDH[video uploading]:
1. Select original video
2. Select target video
3. Check for equisized
4. Divide each frame of video into non-overlapping blocks
5. Block pairing
6. Encrypt data using AES algorithm and embed it into video using RDH
7. Upload video on cloud

4. To download video:
1. Get target video
2. Divide video into frames
3. Anti transformation
4. Get frames of original video
5. Download video frames

V. ALGORITHM

1. Procedure of Transformation

Input: An original image I and a secret key K.

Output: The encrypted image E(I).

Processing:

1. Select a target image J having the same size as I from an image database.
2. Divide both I and J into several non-overlapping 4 * 4 blocks. Assuming that each image consists of N blocks, calculate the mean and SD of each block.
3. Classify the blocks with % α quantile of SD's and generate CIT's for I and J respectively. Pair up blocks of I with blocks of J according the CIT's as described in subsection III-A.
4. For each block pair (B_i , T_i) ($1 < i < N$), compute the mean difference δu_i . Add δu_i to each pixel of B_i and then rotate the block into the optimal direction θ_i ($\theta_i \in \{0^o , 90^o , 180^o ,270^o\}$), which yields a transformed block T'_i .
5. In the target image J, replace each block T_i with the corresponding transformed block T'_i for $1 < i < N$ and generate the transformed image J'_i .
6. Collect δu is and θ is for all block pairs, and compress them together with the CIT of I. Encrypt the compressed sequence and the parameter by a standard encryption scheme such as AES with the key K.
7. Take the encrypted sequence as accessorial information (AI), and embed AI into the transformed image J' with an RDH method and output the encrypted image E(I).

2. Procedure of Anti-transformation

Input: The encrypted image E(I) and the key K.

Output: The original image I.

Processing:

1. Extract AI and restore the transformed image J' from E(I) with the RDH scheme .
2. Decrypt AI by AES scheme with the key K, and then decompress the sequence to obtain CIT of I, δu_i , θ_i ($1 < i < N$) and α.
3. Divide J' into non-overlapping N blocks with size of 4 * 4. Calculate the SDs of blocks, and then generate the CIT of J' according to the %α quantile of SD's.
4. According to the CIT's of J' and I, rearrange the blocks of J' as described in Subsection III-A.
5. For each block T'_i of J' for $1 < i < N$, rotate T'_i in the anti-direction of θi , and then subtract δu_i from each pixel of T'_i , and finally output the original image I.

VI. MATHEMATICAL MODEL

Table 1: Math Model

Set of Inputs	WHERE ,
I = { Oimg , Timg , Ovdo , Tvdo , K }	Oimg = Original Image
	Timg = Target Image
	Ovdo = Original Video
	Tvdo = Target Video
	K = Key for encryption which turns original image into target image
Set of functions	
F = {F1, F2, F3 , F4, F5 , F6 , F7 , F8 , F9 , F10 , F11 , F12 , F13 , F14 , F15 , F16 , F17}	
	F1 = Registration
	F2 = Login
	F3 = Key Generation
	F4 = Non-Overlapping Block Creation
	F5 = Block Pairing Function
	F6 = Block Transformation
	F7 = Upload Image
	F8 = AES encryption

	function
	F9 = Embed Data Function
	F10 = Download Function
	F11 = Video Frame Creation
	F12 = Video Constructor
	F13 = Video Non-overlapping block creator function
	F14 = Video Block Pairing
	F15 = Video Block Transformation
	F16 = Video Upload
	F17 = Video Download
Set of Outputs	
O ={ Ei , Ev}	Ei = Encrypted Image
	Ev = Encrypted Video

VII. EXPERIMENTAL SETUP

System is implementing on java-jdk 1.7.0 platform. Apache-7 and mysql-5.6 is configured on same system at server side. Netbeans 8.0.1 IDE is used for implementation of client side system, it is designed using swing components whereas, and Eclipse indigo is used for cloud server system implementation.

Dataset used:

Equi-sized images are used for image encryption part so that result parameters can be analyzed properly. Following are the image dataset details.

Dataset Name [14]: INRIA Holidays dataset

This dataset is collection of images (photographs) when users / data contributors are on their holidays.

Video dataset[15] consists of various category video clips. For system testing we have downloaded 25fps videos.

VIII. RESULT TABLE AND DISCUSSION

a)Original Image

b)Target image

Images information i.e. Metadata Text message

c)Metadata

d) Encrypted Image

Figure 2: Experimental set up of test images

As per objectives of proposed system, original image (a) is encrypted before uploading it on cloud server. The process of image encryption is begin by adding both original and target image into system. Both get verified by system, for their equality, if both having equal size then two splits are generated. Furthermore, metadata of each image is generated and preserved which is mandatory for image retrieval. After processing combined image i.e. encrypted image is generated. It contains original and target or covered images with their Meta information.

TABLE I: IMAGE PROCESSING

Image Resolution	Processing time in sec.
614x874	0.265
874x1240	0.451
1240x1748	0.549
1748x2480	0.714

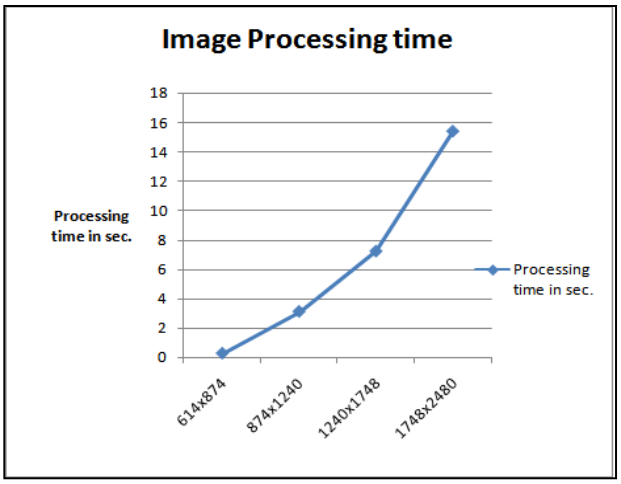

Figure 3: Graph of image processing

We have evaluated proposed system results in terms of image and video processing. In image processing time is evaluated as per resolution of image. According to table I, processing time get increased with increased resolutions of image. It's graphical format is depicted in figure 3 in which X-axis represents image resolutions and Y-axis represents their processing time in second. The processing time consists of image splitting, metadata generation and encryption, RDH.

TABLE II: VIDEO PROCESSING TIME

Video size in MB	Processing time in sec.
4	85
8	180
12	375
15	584

Applying RDH on video is the contribution in proposed system. In table II time required for input video processing before uploading it on cloud server is shown. The processing timing consists of video frame conversion, their splitting, metadata generation and encryption, RDH. Compared to image processing, it required more time due to video frame conversion. In figure 4 graphical form of video processing is shown.

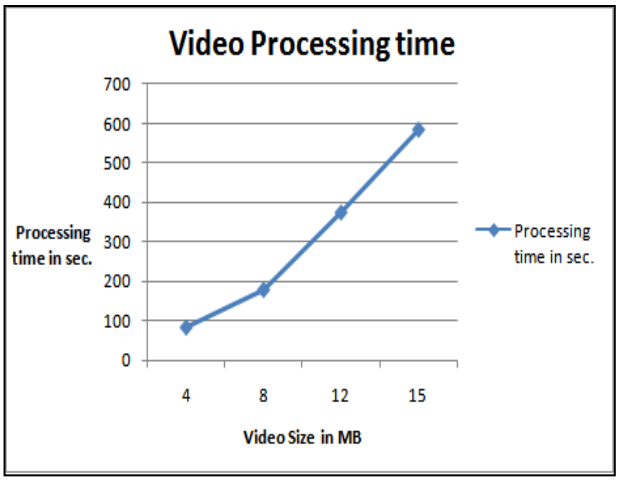

Figure 4: Graph of video processing

It consists of video size in MB on X-axis and processing time in seconds on Y-axis.
For testing we have used videos having 25fps frame rate.

TABLE III: PAYLOAD VS. PSNR

Payload	PSNR
0.05	50
0.1	42
0.15	37
0.2	31
0.25	29

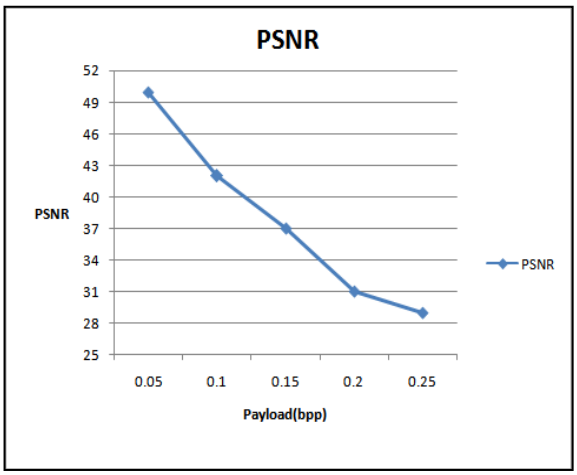

Figure 5: Evaluation of PSNR

Basically PSNR is the Peak-signal to noise ratio. It is used for measuring the quality of reconstructed image. In case of proposed system, we have measured PSNR with the original images.

IX. CONCLUSION

In proposed work, RDH-EI based RIT is proposed. Traditional approaches of hiding data into reversible image such as, RDH, embedding key, HCSRDHEI, RIDH works efficiently to hide or encrypt data to image and extract it from image. These approaches work on data embedding and extracting but the proposed RDH-EI aims to protect outsourced embedded data in cloud environment. It improves image transformation technique. In this original image is transformed

into lossless encrypted image. To enhance quality of image and embedding capacity two existing approaches are utilized namely, PEE-based RDH and USE. PEE is predicted error expansion in this new local least square (LLS) predictor with high prediction accuracy is predicted whereas; UES is unified embedding and scrambling on encrypted image. As a part of contribution data hiding in reversible video is also provided.

VI. REFERENCES

[1] K. Hwang, D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, Sept.-Oct. 2010.
[2] F. Bao, R. H. Deng, B. C. Ooi, et al., "Tailored reversible watermarking schemes for authentication of electronic clinical atlas," IEEE Trans. on Information Technology in Biomedicine, vol. 9, no. 4, pp. 554-563, Dec. 2005.
[3] F. Willems, D. Maas, and T. Kalker, "Semantic lossless source coding," 42nd Annual Allerton Conference on Communication, Control and Computing, Monticello, Illinois, USA, pp. 1411-1418, 2004
[4] W. Zhang, X. Hu, N. Yu, et al. "Recursive histogram modification: establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. on Image Processing, vol. 22, no. 7, pp. 2775-2785, Jul. 2013.
[5] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. on Circuits and Systems for Video Technology, vol.19, no.7, pp. 989-999, Jul. 2009
[6] Ioan-Catalin Dragoi, Dinu Coltuc, "Local-prediction-based difference expansion reversible watermarking," IEEE Trans. on Image Processing, vol. 23, no. 4, pp. 1779-1790, Apr. 2014
[7] X. Hu, W. Zhang, X. Hu, N. Yu, X. Zhao, F. Li, "Fast estimation of optimal marked-signal distribution for reversible data hiding," IEEE Trans. on Information Forensics and Security, vol. 8, no. 5, pp. 779-788, May. 2013.
[8] W. Zhang, X. Hu, N. Yu, "Optimal transition probability of reversible data hiding for general distortion metrics and its applications," IEEE Trans. on Image Processing, vol. 24, no. 1, pp. 294-304, Jan. 2015.
[9] J. Zhou, W. Sun, L. Dong, et al., "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 3, pp. 441-452, Mar. 2016.
[10] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. on Information Forensics and Security, vol. 7, no. 2, pp. 826-832, Apr. 2012.
[11] Z. Qian, and X. Zhang, "Reversible data hiding in encrypted image with distributed source encoding," IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 4, pp. 636-646, Apr. 2016.
[12] W. Zhang, K. Ma and N. Yu, "Reversibility improved data hiding in encrypted images," Signal Processing, vol. 94, pp. 118-127, Jan. 2014.
[13] X. Cao, L. Du, X. Wei, et al., "High capacity reversible data hiding in encrypted images by patch-level sparse representation," IEEE Trans. on Cybernetics, vol. 46, no. 5, pp. 1132-1143, May. 2016.
[14] http://lear.inrialpes.fr/people/jegou/data.php
[15] https://www.videvo.net/stock-video-footage/video

