JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Research Paper on Enhancing Cloud Data Security using Watermarking Technique

Arpita Sinha[1], Sudhir Goswami[2], Dr Kirti Jain[3]

[1] Research Scholar, [2] Asstt Professor, [3] Head of Department

[1]Computer Science and Engineering

[1]School of Research and Technology, People's University, Bhopal (M.P.) India

Abstract: **Nowadays info security is on its prime priority for all organizations. The cloud storage provides knowledge storage facilities similarly as sharing across multiple users. It is gaining quality as a result of monumental edges. The people, government, and military with the speedy development of new technologies just like the net of Things, big data, and cloud computing facing knowledge security issues. With the huge rate of information growth, it's a difficult task the way to manage the large quantity of information safely and effectively. It's been quite simple to provide associate banned copy of digital contents. The verification of digital content is one amongst the most important problems as a result of digital contents ar generated daily and shared via the web. However rising knowledge security and privacy problems has become a topic of primo to the users similarly because the service suppliers. This paper addresses the safety problems and proposes cloud based mostly digital watermarking approach. The cloud based digital watermarking application extremely protractible wide shareable, and safer. The watermarking technology takes under consideration the invisibleness and lustiness of the watermark by dominant the embedding intensity and position of the watermark primarily within the transformation domain. The projected technique is strong and resists from info attacks and capability of the projected technique is additionally improved as compared to the previous techniques.**

***Keywords*— Information Security, Storage, Cloud, Attacks, digital watermarking, Privacy.**

I. INTRODUCTION

Nowadays cloud computing is increasing technology thanks to its Brobdingnagian usages. Cloud storage services alter users to source their information to cloud servers and access that information remotely over the web. These services provide users associate economical and flexible manner to manage their information while not deploying and maintaining native storage devices and services. Users will method their information on their PCs, source the processed information to cloud servers and use the information on alternative devices. The use of mobile device to access and share transmission content such as pictures, video, transfer of code applications, pay on-line bills and communicate on the cloud over the net is increasing with the forceful growth in transmission technology [11]. In cloud computing, cloud information storage contains 2 entities as cloud user and cloud service provider cloud server. Cloud user could be a one who stores great amount of information on cloud server that is managed by the cloud service supplier. User will transfer their information on cloud without concern concerning storage and maintenance. A cloud service supplier can offer services to cloud user. the foremost issue in cloud information storage is to get correctness and integrity of information keep on the cloud. Cloud Service supplier has to offer some type of mechanism through that user can get the confirmation that cloud information is secure or is keep as it is. The cloud information storage service contains three completely different entities as cloud user, Third party auditor & cloud server / cloud service supplier. Cloud user is a person UN agency stores great amount of information or files on a cloud server. Cloud server could be a place wherever we have a tendency to are storing cloud information and that information are going to be managed by the cloud service supplier. Third party auditors can do the auditing on users request for storage correctness and integrity of information. The cloud atmosphere is vulnerable to completely different attacks that ar giving a negative mark to impede the trust in adopting cloud computing. External and internal attacks are known as a threat to cloud infrastructures. Security in cloud computing is self-addressed in several ways that as authentication, integrity, confidentiality. information integrity or information correctness is another security issue that desires to be thought of. information on the cloud are sensitive and non-public. moreover, any bootleg access to these information could lead to privacy violation, outpouring or injury of sensitive information. to realize information confidentiality, integrity and availableness of the transmission information in the cloud the use of security techniques such as cryptography, steganography and watermarking are used to shield the information from bootleg access by malicious users and hackers.

Overview of Watermarking

Watermarking methodology being enforced on the text files for information leak detection. The watermark is applied on the numerous components of the files and later sends to the requested Agent. On finding the distinctive watermark at a unauthorized person or a firm will be thought-about as information leak scenario. Watermarks can be of the text, audio and image sorts. These are often watermarked victimization specific acceptable strategies. General text files will be watermarked with regular text in background. pictures will be watermarked using the Cocktail Watermarking and Robust Watermarking methodologies. Cocktail watermarking are often wont to alter the image victimization the moving ridge coefficients specially areas of pictures.

Digital Watermarking

Digital watermarking is a security technology that embeds signals and Secret data known as watermarked at intervals digital media content such as image, audio and video. It ensures security, privacy and ownership authentication of the media content being watermarked. The thought behind watermarking is connected to steganography. Steganography is outlined as secret writing, that is used for secret communication in while history. Digital watermarking is employed to cover un-perceptible label or mark on a media content that may later be detected and extracted by a licensed user in order to defend product copyright or media information integrity. There square measure two sorts of digital watermarking techniques, the visible and invisible. The visible watermarking technique is that the one we are able to see and spot on product or emblem on our tv. While, the invisible watermarked is the one that is un-perceptible by human eyes. The invisible watermarking is categorised into weak and sturdy watermarking. The fragile watermarking is used to verify the integrity of a media content as a result of any slight modification created on fragile watermarking media content produce some changes to the original meantime, the sturdy watermarking technique is used to manifest the proof of possession of the aforesaid media content . The advantage of the sturdy reversible watermarking techniques is that it permits the extraction of the complete content of the media content being watermarked whereas not poignant it

II. BACKGROUND AND RELATED WORK

H. Geet. al. [1], Proposed a DCT based watermarking technique. In spatial domain and transform domain with respect to imperceptibility, capacity, robustness, security and complexity. Taking the benefits of energy compaction property, robustness of JPEG compression attacks and good performance in perceptual transparency is more reliable for many application. DCT shows a good performance in case of hardware design, performing lower price and better throughput contrast to DWT, mainly because of lower computational complexness.

A. K. Singh [2], proposed a multiple image watermarking approach where LWT along with DCT is employed. In this methodology a coloured host image is converted from RGB to YIQ color space. Further 'Y' component is chosen for embedding of watermark while 2 encrypted watermarks are embedded concurrently inside the host image. Developed technique seems to be robust against varied attacks and provides adequate security to the watermarks.

L. Tanwar et. al.[3], stated that robust watermarks are required to remain in the watermarked image even after it has been manipulated by different attacks whereas the fragile watermarks are designed to be broken easily by image processing operations. In addition, digital watermarking technology can be classified by diverse domains, i.e., spatial domain, transformation domain and compression domain.

Arora et al. [4], evaluated steganography techniques from other metrics such as perceptual transparency and computation complexity. All of these properties connect each other that is an increase in the payload capacity results in a decrease in the imperceptibility of the secret watermark data. Also decrease in the capacity improves the robustness. They have researched plenty of comparative studies to provide a general overview of four methods, which are most common used in watermarking techniques.

Chang et al. [5], employ both online and offline content-adaptive predictors to assist watermark decoding for various operational requirements. When an illegal image is found, by the watermark extraction method an unauthorized user can be created public. Privacy-aware reversible watermarking permits a celebration to entrust the task of embedding watermarks to a cloud service provider without compromising information privacy.

Khare et al. [6] planned a method during which reflectance component of host image is processed with DWT and watermark is directly added to SVs of reflectance component of LL sub-band. It appears that this reported method attains better robustness and imperceptibility due to use of DWT which provides sub-band analysis of reflectance component.

A. Zear et.al. [7], proposed dual image watermarking methodology where two watermarks are simultaneously embedded inside a medical host image. In this approach host image is decomposed upto 3rd level DWT, followed by DCT and SVD. Similarly both watermarks are also processed by DCT and SVD. SVs of first watermark are embedded into SVs of LH2 sub-band of host image whereas SVs of second watermark are altered with SVs of LL3 sub-band. To enhance robustness of algorithm back propagation neural network is applied.

L. Singh et. al [8], elaborated several watermarking techniques where authors have highlighted the salient features of numerous watermarking techniques. This actually helps researchers in providing roadmap for developing new watermarking methodologies. Researchers have proposed a novel dual image watermarking technique where RDWT, NSCT, AT and SVD transforms are effectively used. Dual image watermarks are embedded in this methodology whereas set partitioning in hierarchical tree (SPIHT) algorithm is employed successfully for compressing the watermarked image.

P.Saranyaet. al.[9], propose the methodology in which the finger print image which is obtained from the user is Steganographed with PIN NUMBER of the user and the Steganographed image which in turn is divided into two shares. One share is stored in the bank database and the other share is provided to the customer. Hash code is generated for the customer share and it is stored in the One Time Password (OTP) is used every time to ensure the trusted submission of shares. This has the earliest method of sharing secret codes and message. This proposed approach is aimed to made several implementations to increase the data security and user authentication is the arena of visual cryptography.

G. Preethiet. al.[10],proposed a method to protect medical images stored in cloud using Reversible Data Hiding by improving image quality and cloud capacity. The data along with a cover image is split into matrix format and is encrypted using asymmetric key. The cells are decrypted using Reversible Data Hiding Techniques.

Monisha et. al.[11], proposed an enhanced security technique to have a secure communication of data in the cloud over the internet using RSA digital signature with robust reversible watermarking algorithm. In their work, RSA was used to encrypt and decrypt the multimedia content using its public and private keys and hash function was used to reduce the size of the multimedia content to any size called hash value and to also, sign the multimedia content for authentication and validation. In order to prevent the security challenge of insider attack on user data in the cloud by cloud service provider administrator.

S. Gaur et. al[12], investigated major difference lying in both schemes is use of image transforms. In this approach redundant discrete wavelet transform (RDWT) is employed whereas DWT is used for decomposing the cover image. In this methodology secondary watermark is embedded inside a primary watermark, afterwards SVs of new primary watermark are inserted into SVs of cover image. However, this method does not yield sufficient value of correlation co-efficient.

Assini et al. [13], developed multiple image watermarking method using fusion of DWT – fast Walsh Hadamard SVD. SVs of various watermarks were embedded into SVs of host image in this scheme. In this procedure different watermarks are embedded into a host image with aim of maximizing certain objective function, so that scheme can become more robust and imperceptible.

Preetet. al. [14], proposed a multiple image watermarking technique for color images where two image watermarks are concurrently embedded inside a color host image. In this approach, a RGB colored host image is transformed into color space. Further 'Y' component is decomposed up to 2nd level using lifting wavelet transform (LWT) where LL2 and LH2 sub-bands are further transformed by DCT. DCT is also applied on both the water-marks, out of which first watermark is encrypted through AT. Finally these DCT transformed watermarks are embedded into host image.

Kaur et al. [15] established a new approach of watermarking with the help of dual tree complex wavelet trans-form (DTCWT) and AT. A host image is decomposed into various sub-planes using DTCWT whereas encrypted watermark image is also decomposed in a similar manner using DTCWT while encryption of watermark is done through AT. Further embedding process is performed for all sub-planes distinctively whereas inverse DTCWT leads to generation of watermarked image. However, the developed scheme turns out to be a non-blind schemewhich requires original host image for recovery of watermark.

Uma et. al.[16], proposed a solution to the security threat and fear faced by cloud users using robust reversible watermarking and RSA digital signature. It was stated in their work that due to the limitation of the traditional watermarking technique in distorting the water marked objects and not able to extract it full content back the need to use the robust reversible watermarking in protecting data on the cloud. Two security methods reversible watermarking and RSA digital signature were used to improve confidentiality and cloud security level between mobile user and mobile cloud environment when sending information to the mobile cloud service providers in their work. Due to rise in technology and increase transfer of multimedia content son the cloud using mobile devices.

Mbarek Marvanet. al[17], explained that using two-out-of-two visual cryptography a digital record is split into two records. To ensure security each split is stored at different cloud locations. This work explains the concept of multi cloud environment and the storage of data in multi cloud environment which reduces the data vulnerabilities and security risks involved in a single cloud system.

Sathishkumaret. al[18], proposed a method to perfectly restore the color images using two in one Image Secret Sharing Scheme (TiOISSS). The extension of TiOISSS for color images was performed to improve the quality and construct the image perfectly. The RGB components were extracted for share generation. The extracted components were permuted three times by attaching a key to improve the security. During decryption the authenticity is checked using the keys.

SiddhantBansalet. al [19], Analyzed various watermarking techniques and joint encryption algorithms used to secure biomedical images. Hence the detailed summary of different technique of watermark and joint encryption is presented.

Pei-Ling et. al[20], proposes a methodology. This methodology proposes a (2, n) XFPVCS to share a binary secret image for n participants. The experiments show that the proposed encryption method has following advantages. The algorithm is a systematic approach for pixel-expansion-free (n, n) XFPVCSs. It provides an adjustable visual quality of meaningful shares.

Priyankaet. al.[21], proposed the storage of document in cloud that is encrypted using AES. An order preservation encryption(OPE) key is generated which is used to authenticate the user. This generated key is matched with the users OPE and the user is verified. Decryption is done using the same generated key. This ensures security, efficiency and accuracy to the document.

Vandana Purushothaman et.al[22],proposed a method to reduce pixel expansion during the process of visual cryptographic share generation using XOR operation by preserving the image quality. The method consisted two phases including a share generation phase and hiding phase. Shares are generated using XOR operation avoiding the pixel expansion. Then the generated shares are hided using another image using steganography which gives additional security to the original image.

III. SYSTEM MODEL

Cloud users face severe security challenges from each within and out of doors the cloud. The paper proposes watermarking techniques that have two phases to secure the shared knowledge objects in cloud computing. 1st is to implant the visible watermark which might be seen by everyone World Health Organization is seeing the information object. Second is to insert the hidden watermark that provides backup facility just in case once visible watermark fails to prove trustiness of knowledge. Both visible and hidden watermarks area unit embedded within the knowledge objects once these knowledge packets area unit

created or additional for the primary time within the cloud. the method of embedding each visible and hidden watermarks within the host knowledge object consists of two steps as shown in Figure.1 and therefore the experiment is performed with six totally different pictures victimization own-Cloud. The own-Cloud infrastructure is put in at a centralized server laptop and organized with a static IP address. Totally different styles of nodes or shoppers like desktop computers, mobile phones, associate degreed laptops area unit deployed in a very network and these shoppers will access the own Cloud interface through an IP address.

IV. RESULT AND ANALYSIS

In visualize performing the experiment the complete image is separated into three rectangles. The hidden watermark in inserted into the innermost parallelogram whereas visible watermark is placed into the outer parallelogram adjacent to the outmost boundary of the image.

xi = (x i-1)/ (i x 10) (1)

yi = (y i-1)=(i x 10) (2)

Where, i >=1, x0, and y0 is width and height of original image, respectively.

$\sum_{i=1}^{l} x\ i$, $\sum_{i=1}^{l} y\ i$ (3)

$xb = \sum_{i=1}^{l} x\ i$, $yb = \sum_{i=1}^{l} y\ i$ (4)

Where, i >=1, Equation (1) calculates the breadth of inner parallelogram that is reduced by common fraction w.r.t the breadth of outer parallelogram, whereas (2) calculates height of inner parallelogram. After calculative the gap from outer most layers, coordinates of initial and last purpose of inner parallelogram area unit calculated in (3) and (4). During this approach, the total space of the image is divided into 3 parallelograms and each visible and invisible watermarks area unit embedded in outer and inner rectangle, severally.

Sr. No	without watermark	with watermark
1	0	0.27
2	0	0.31
3	0	0.33
4	0	3.57
5	0	5.98
6	0	7.65

Table1: Image Upload time in cloud (Sec)

V. CONCLUSION

Cloud computing ideally thought of next-generation design thanks to dynamic resource pools, low cost, responsibleness, virtualization, and high convenience. In cloud computing, one necessary issue is to trace and record the origin knowledge of information objects that is understood as data cradle. Major challenges to cradle management in distributed surroundings area unit privacy and security. So as to trust on the cloud information, there's a requirement to trace the origin of information object. To handle this downside, a watermarking technique is planned that stores the knowledge regarding the origin of information product. This method uses two necessary forms of watermarks that area unit visible watermark and hidden watermark. By adopting this technique, shared information object within the cloud will be safe from the malicious attack which will amendment or lose the important possession of that information object. Finally, the potency and responsibleness of this adopted approach is evaluated by conniving the time needed to insert each visible and hidden watermarks on information objects. During this paper the matter of information cradle is targeted at intervals a same cloud computing surroundings. Within the close to future, another techniques area unit expected to confirm the trait of shared information objects among totally different cloud computing environments.

REFERENCES

[1] H. Ge and J. Sha, ``FPGA-based low-complexity high-throughput real-time hardware accelerator for robust watermarking," J. Real-Time Image Process., vol. 16, no. 4, pp. 813820, Aug. 2019.
[2] A. K. Singh, Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image, Multimedia Tools and Applications. (2019), 1-11.
[3]L. Tanwar and J. Panda, ``Review of different transforms used in digital image watermarking," in Proc. 2nd IEEE Int. Conf. Power Electron., Intell. Control Energy Syst. (ICPEICES), Oct. 2018
[4] H. Arora, C. Bansal, and S. Dagar, ``Comparative study of image steganog-raphy techniques," in Proc. IEEE Int. Conf. Adv. Comput., Commun.ControlNetw. (ICACCCN), Oct. 2018, pp. 982985.
[5]C.-C. Chang, C.-T.Li, and Y.-Q. Shi, ``Privacy-aware reversible water-marking in cloud computing environments," IEEE Access, vol. 6,pp. 7072070733, 2018.
[6] P. Khare and V. K. Srivastava, Image Watermarking Scheme using Homomorphic Transform in Wavelet Domain, in: 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), pp. 1-6, IEEE, 2018.
[7] A. Zear, A. K. Singh and P. Kumar, Multiple watermarking for healthcare applications, Journal of Intelligent Systems. 27 (2018), 5-18.
[8] L. Singh, A. K. Singh and P. K. Singh, Secure data hiding techniques: a survey, Multimedia Tools and Applications. (2018), 1-21.
[9] P.Saranya, Dr.M.Vanitha," User Authorization with Encrypted Visual Cryptography Using High Definition Images", International Journal of Pure and Applied Mathematics,Volume 118 No. 8 2018, 429-433
[10]. G. Preethi and N.P.Gopalan," Data Embedding into Image Encryption using the Symmetric Key for RDH in Cloud Storage", International Journal of Applied Engineering Research ISSN 0973-4562, Volume 13, Number 6 (2018) pp. 3861-3866,2018.
[11]Anuradha, A., &Pandit, H. .(2017). Biometric Based Security Model for Cloud Computing Using Image Steganography. International Journalof Advanced Research in Computer Science and Software Engineering, 7(1), 42-51.
[12] Apau, R., &Adomako, C. (2017). Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones. International Journal of Computer Applications, 164(1), 13-22.
[13] Monisha, M., & Chidambaram, S.(2017). Enhanced Data Security usingRSA Digital Signature with Robust Reversible Watermarking Algorithm in Cloud Environment. International Journalof Electronics& Communication Technology, 8(1), 20-24.
[14]S. Gaur and V. K. Srivastava, A RDWT and Block-SVD based Dual Watermarking Scheme for Digital Images, International Journal of Advanced Computer Science and Applications. 8 (2017), 211-219.
[15] Assini, A. Badri, K. Safi, A .Sahel and A. Baghdad, Hybrid multiple watermarking technique for securing medical image using DWT-FWHT-SVD, in: Advanced Technologies for Signal and Image Processing(ATSIP), 2017 International Conference on. pp. 1-6, IEEE, 2017.
[16] Preet and R.K. Aggarwal, Multiple image watermarking using LWT, DCT and Arnold transformation, in: 2017 International Conference on Trends in Electronics and Informatics (ICEI), pp. 158-162, 2017.
[17] S.Kaur and R. Talwar, Arnold transform based Security Enhancement using Digital Image Watermarking with Complex Wavelet Transform, International Journal of Electronics Engineering Research.9 (2017), pp. 677-693.
[18] Uma, B., &Sumathi, S. (2017). An Efficient Approach for Data Security in Cloud Environment using Watermarking Technique and RSA Digital Signatures. International Research Journal of Engineering and Technology, 4(2), 1817-1821
[19]MbarekMarvan, Ali kartit, Hassan Ouahmane,"Protecting Medical Images In Cloud Using Visual Cryptography Scheme", International Conference of Cloud Computing Technologies and Applications (CloudTech) , 2017
[20] R. Sathishkumar andGnanou Florence Sudha, "Authenticated Color Extended Visual Cryptography withPerfect Reconstruction", International Conferenceon Communication andSignal Processing, 2017.
[21].SiddhantBansal and GarimaMehta, "Comparative Analysis of joint encryption and watermarking Algorithms for security of Biomedical Images", 7th InternationalConference on Cloud Computing,Data Science & Engineering – Confluence, 609978-1-5090-3519-9,2017
[22]Pei-Ling Chiu, Kai-Hui Lee, "An XOR-based Progressive Visual Cryptography with Meaningful Shares", IEEE International Conference on Computer Communication and the Internet (ICCCI), 2016
[23]Priyanka.K, Mrs.V.MercyRajaselvi M.E, "secured document search and retrieval using visual cryptography scheme in cloud environment", International Journal of Computer Technology & Applications, Vol. 7(3),458-464,2016
[24]VandanaPurushothaman, SreelaSreedhar, "An improved secret sharing using xor-based visual cryptography", Online International Conference on Green Engineering and Technologies (IC-GET), 16864747,2016