EasyChair Preprint

№ 3027

Data Integrity and Security in Distributed Cloud Computing: A Review

Abdullatif Ghallab, Mohammed Hamood Saif and Abdulqader Mohsen

March 22, 2020

Data Integrity and Security in Distributed Cloud Computing: A Review

Abdullatif Ghallab[1*], Mohammed H. Saif[2], and Abdulqader Mohsen[1]

[1]University of Science and Technology, Sana'a, Yemen

[2]University of Science and Technology, Taiz, Yemen

ghallab@ust.edu, m.naji@ust.edu, a.alabadi@ust.edu

Abstract. Data storage of cloud services have increased rates of acceptance due to their flexibility and the concern of the security and confidentiality levels. Many of the integrity and security problems raised based on the differences between client and service provider for resolution of third-party auditor. This review paper gives a brief view of current data integrity and security issues in the distributed cloud computing environment. The paper compared eight different models of the cloud data integrity and security. It highlights nearly solutions for some of the current cloud security risks and challenges by summarizing the key schemes of the privacy preserving public auditing, particularly access control, attribute-based access control, and public key encryption. Moreover, the paper assigning the existing models, algorithms, and methodologies of data integrity and security done in the literature of distributed cloud security. It suggested further research in cloud security domain regarding many of the security and data integrity issues.

Keywords: Cloud Security, Distributed Cloud, Data Integrity, Auditing Schemes, Privacy Features.

1 Introduction

The rapid development in networking technology and the variation of computing resources requirements have enforced companies to outsource their needs of storage and computing services. In the new economic, cloud computing encompasses different kinds of services. With the infrastructure as a service (IaaS) mode, clients use computing services from a provider through internet. They are in charge of storage, as well as for the networking infrastructure. In the platform as a service (PaaS) mode clients use the resources of the provider for running their custom apps. Whereas, in the software as a service (SaaS) clients uses the software, which runs on the infrastructure of the providers.

Cloud infrastructures may fall in the private group or in the public group. A private cloud refers to on in which the customer does management of the infrastructure. The customer is the owner. At the same time, the location is on premise. It also implies that the client is capable of controlling access to data. Access can be given to the people who are trusted. When it comes to public cloud, the company providing the service is the one, which owns and manages the infrastructure. The location of the infrastructure is on-premise of the company providing the service. Generally, a different party is managing client information. Whereas untrusted parties capable of gaining access to the data.

Storage services like Microsoft's Azure and Amazon's S3 offer clients through storage, and can be scaled dynamically. Moving the data of clients into the cloud required different kinds of cost with ensuring a proper maintenance of their private storage infrastructure. This made them to resort to other service providers at a fee to meet their storage needs. For a number of the customers, it generates numerous

advantages, which generally includes the fact that they are readily available. The clients are capable of accessing the data at any time from any point. The other major advantage is the fact that they are highly reliable. This generally implies that the customers do not have to be worried concerning anything like backups.

2 Review of Literature

A model proposed by [1] called “provable data possession (PDP)”. The key feature of this model is verification of data on an untrusted server without retrieving. This is done by generating probabilistic proofs of blocks and maintaining metadata of the proof; also, the response protocol is small and constant reducing network communication. The PDP model with two schemes can support huge data in distributed systems with lower overheads at server level and the performance being dependent on disk I/O. In [2] a proposed model emphasis on third-party auditing to enable customers assessing risks and the associated insurance risk mitigation. The focus was on both internal and external auditing of storage service offered online. This model is aimed at enabling customers to make informed choices give the service providers and auditors to develop approaches for auditing and overcome the challenges.

In [3] improvement of PDP scheme of [1] as “dynamic provable data possession (DPDP)”. The PDP scheme works with only the static files the DPDP scheme by the usage of rank information also supports the updates (apart from static) to the data stored on CSP. The scheme used “Merkle Hash Tree (MHT)” for verification but works only for single file copy and are not encrypted. By adopting 's protocol a model proposed by [4] using PDP scheme. The key feature of this scheme is public verifiability for the data stored on CSP. The public verifiability is done by a TPA without the exposing the information of the data owner. This model did not consider data encryption and is limited to single data files. A PDP scheme proposed by [5]. The key aspect of this model was the usage of FHE algorithm for data file encryption. The benefit of this feature is it generated multiple copies on the CSP and whenever the file copies were updated, they do not require re-encryption. Two PDP schemes were proposed in this paper that enabled CSP to store lesser and fewer copies of files and adopt the dynamic behavior on cloud servers for data copies modifications. The model provided a solution to reduce storage costs and storage space requirements.

The key features of the privacy preserving and public auditing which summarized from literature are shown in Figure 1.

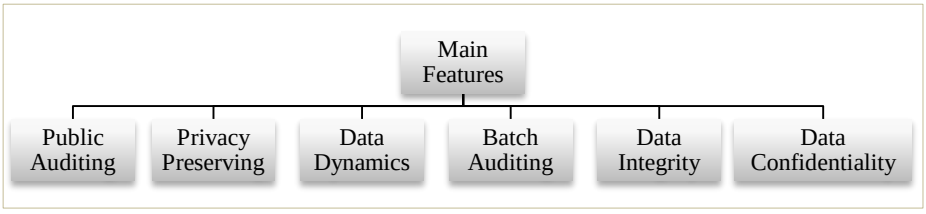

Fig. 1. Main features of the privacy preserving and public auditing

In [6] proposed a “proofs of retrievability (POR)” technique based on two schemes. The first is modeled with shortest query and response with public verifiability built from BLS signatures. The second is modeled on shortest response with private verifiability built on pseudorandom functions (PRFs). The model enables the client’s data to any prover passing the authentication check. In [1] proposed PDP technique for integrity of storage. The key focus is a third-party auditor (TPA) acting for a client to verify the data on the cloud dynamically. Cloud is not only limited to data backup but also involves block modification, insertion and deletion. The model improvised on Merkle Hash Tree (MHT). The model works for block authentication and dynamic public verifiability. The [7] as compared to [6] introduced a model of compact “proofs

of retrievability (POR)" scheme. The TPA's role has been better focused by eliminating the need for local copy of data thereby reducing the role of cloud user and removing vulnerabilities of user data privacy. The model integrates homomorphic authenticator along random masking. The feature of simultaneous multiple auditing is also added with a multi-user setting. Public verification schemes have been proposed in [8] and [9] based on [7] model with a homomorphic signature, a trusted TPA and certificate-based cryptography.

The work [9] with a solution of POR for dynamic storage, focused on a scheme against malicious auditor by the technique of oblivious RAM. In this model the client is enabled to execute arbitrary reads/writes and audits in their data with a protocol on the server to check/ensure the latest version. In [10] a dynamic POR scheme ensuring client storage is proposed in a cost-effective way as compared to Merkle Hash Tree (MHT). The model outperformed two dynamic POR schemes namely (ACSAC 2012) and (EUROCRYPT 2013). Further [11] proposed a PDP scheme to support the dynamic authentication. Further dynamic authentication schemes have been proposed in [12], [13] and [14].

In [15] introduced a protocol by utilizing the services of a TPA. The method called as privacy preserving auditing employs homomorphic linear authenticator (HLA) and random masking. The shortcomings in this model noticed are message attacks and external attacks. To overcome the shortcomings in [15] in [16] introduced an improvised scheme built from "Boneh-Lynn-Shacham signature (BLS)". Though improvised the scheme is not as efficient due to computationally intensive pairing operation. The scheme was implemented on Amazon EC2 but not tested on commercial public cloud making it unsuitable for handling large scale data.

In [17] introduced a protocol with "Merkle Hash Tree (MHT)" along with BLS based HLA. The model works for data dynamics and public auditing. While the model ensured integrity of data it lacked in ensuring confidentiality of cloud stored data. In [18] introduced a design to get the intended blocks from various servers. The model used homomorphic token pre-computation and subsequently coded technique for erasure. In [19] introduced a design that collects signatures on blocks as a bundle. While the security aspect in the model is similar to [16] and ensured better efficiency as compared there was an increase of overhead in communication and computation. In [20] developed a model using Merkle Hash Tree algorithm for TPA of the user's data. While the data dynamics were supported it lacked in ensuring confidentiality of cloud stored data.

In [21] proposed a model of MHT and RSA based cryptography. The model ensured both integrity and privacy of data. In [22] proposed a different model to monitor the data changes on cloud. They placed an attacking module a code on the cloud server that performs the function of monitoring on cloud server while the confidentiality is ensured by employing AES algorithm. In [23] introduced a method of "Hash Message Authentication Code (HMAC)" along with homomorphic tokens. By using a secret key, the integrity of data shared between two entities is ensured. The shortcoming in this model is fraud messages are created by malicious attackers if the secret key is compromised. In [24], [25] introduced a model using a TPA in a privacy preserving public auditing scheme. The user creates the blocks by AES algorithm, assigning hash, sequencing the hashes and generating RSA signature. The TPA ensures the verification of data integrity by signature matching.

A Comparison of the privacy preserving and public auditing models and schemes based on key features of the privacy preserving and public auditing are represented in Table 1.

Table 1. Comparison of the privacy preserving and public auditing schemes

Models	HLA with random masking [15]	HLA with BLS signature [16]	HLA with BLS signature along with MHT [17]	Homomorphic tokens with Erasure code [18]	Merkle Hash tree [20]	MHT and RSA algorithm [21]	HLA with random masking and AES algorithm [22]	HMAC Algorithm [23]
Features								
Public Auditing	√	√	√	√	√	√	√	√
Privacy Preserving	√	√	√	√	√	√	√	√
Data Dynamics			√	√	√			
Batch Auditing		√	√				√	
Data Integrity	√	√	√	√	√	√	√	√
Data Confidentiality						√	√	

Among the eight models included in the comparison, two models satisfy 5 among 6 features, HLA with random masking and AES algorithm [22], HLA with BLS signature along with MHT [17], all features except data confidentiality, and data dynamic, respectively. The next rank of four models that achieved 4 features. All the four models satisfied the same three features, public auditing, privacy preserving, and data integrity, whereas two of them satisfied data dynamic. A different single one feature only, batch auditing, and data confidentiality, was satisfied by HLA with BLS signature [16], and MHT and RSA algorithm [21, respectively. Finally, both HLA with random masking [15], and HMAC Algorithm [23] models satisfied the lowest rank with similar three features: public auditing, privacy preserving, and data integrity.

Figure 2 illustrates three key schemes of the privacy preserving public auditing. It is noted well that the majority of models for privacy preserving public auditing, exposed in Table 1, depend on the three schemes: access control, attribute-based access control, and public key encryption. The following sections review the main features of each scheme.

Fig. 2. Key schemes of the privacy preserving and public auditing

2.1 Access Control

Access control is a key feature for trusted security in cloud storage services. This requirement has evinced research interest from the academia and the industry. In [26] the researchers used a combination three encryptions for cloud access security. In the model the access rules were defined based on data characteristics and the owner of the data can assign tasks in cloud servers without opening the actual content. In [27] as compared to "Hierarchical Attribute-Based Encryption (HABE)" a low communication and computing cost attribute-based system was developed. The data access control is through user attribute rules and authentication is through identity-based signature.

In [28] broadcast encryption approach was adopted with a focus on smaller

enterprises that are constrained by tight budgets and aid in cost savings by productivity enhancements. The model uses a combination of “hierarchical identity-based encryption (HIBE)” system and the “ciphertext-policy attribute-based encryption (CP-ABE)” system. In [29] a model of proxy re-encryption was adopted with patient centric framework. The model leveraged multiauthority “attribute-based encryption (ABE)” for patient health records. The model is also built with dynamic modification of user, attributes and access policies.

In [30] a model of role-based encryption is built called as “hierarchical attribute-set-based encryption (HASBE)”. This model overcomes the shortcomings of attribute-based encryption (ABE) like lack of flexibility or executing complex access policies. HASBE has the ability to employ multiple values for user access management.

In [31] a model of “Multi-message Ciphertext Policy Attribute-Based Encryption (MCP-ABE)” is employed for sharing consumer data attributes excluding the actual names. The benefit of MCP-ABE it enables the content provider to specify the access policy giving the data only to the intended and approved users.

In [32] a model of “Ciphertext policy attribute-based encryption (CP-ABE)” is employed for data sharing. The model enabled to overcome the shortages of key escrow and fine-grained user revocation for each attribute.”.

2.2 Attribute-based Access Control

In [33] the model combined a method of ciphertext delegation enabling it to be ‘re-encrypted’ and provide security in the standard ABE framework. This model enabled in dynamically disqualifying revoked users. In [34] a dynamic policy update is implemented for big data. The access policies in this model are designed for minimal computation for data owners, use of old data and access policies, algorithmic update of policies and check mechanism for update of ciphertexts. In [35] the authors have proposed a scheme where “Ciphertext-policy attribute-based proxy re-encryption (CP-ABPRE)” supports the attribute-based re-encryption. The model is built to overcome “chosen-ciphertext attack (CCA)” securely enabling the scheme to handle the problem.

In [36] a model is “public key encryption (PKE)” proposed to verify two ciphertexts are encryptions of an identical message. The scheme eliminates the need for bilinear map operations except for equality test. The application where PKE is useful are searchable encryption and encrypted data partitioning. Similar kind of PKE schemes have been proposed in [37] and [38].

In [39] a model of identity-based distributed provable data possession (ID-DPDP) is proposed. ID-DPDP protocol is developed on a multi cloud storage and is secure under Computational Diffie-Hellman problem (CDH). The model allows remote data checking without downloading the whole data and reduce the costs. This model is applied for patient records in public cloud under KP-ABE.

CP-ABE characteristics due to their flexibility are more preferred in applications of cloud access control. In [40] to overcome the problem of complicity of data storage a “multiple-replica provable data possession (MR-PDP)” proposed. The storage is done and authenticated by challenge-response protocol. The scheme is economical as compared to single-replica PDP scheme. In [41] a Proofs-of-Retrievability (PoR) is proposed to reduce the computational load by outsourcing files on low-power client’s verifications on high end servers and supporting dynamic updates. Performance analysis was also done for this scheme giving it an upper hand to the compared ones. [42] Also focused on CP-ABE application. In [43], [44] and [45] studies were done on policy updates. The studies had their own shortcomings where they used proxy re-encryption. This does not really update or extend the access policy and lacks integrity of linking to the actual data.

2.3 Public Key Encryption

In [46] the author introduced a public key encryption scheme (PKE). In this scheme the bilinear map operations are required only in the case of equality test of encrypted messages between two ciphertexts. The scheme is useful for encrypted applications like search or partition. The shortcoming observed in PKEET lack of integrity check. In [47] Tang introduced a model enabling two users with public/private key to issue token(s) for equality test between ciphertexts. The model incorporates fine-grained authorization policy. The model is useful for TPA operations. In [48] Tang improvised on [47] fine-grained authorization (FG-PKEET) by working on flaws on equality test, compare with AoN-PKEET by Tang and PKEET by and make FG-PKEET function on a two-proxy setting.

In [49] Wang keeping in view the aspects of verification, multi cloud storage and costs proposed an identity-based distributed provable data possession (ID-DPDP) in multi cloud storage. ID - DPDP protocol is made on bilinear pairings and secure under standard CDH problem. The ID-DPDP protocol functions for private, delegated or public verification. The shortcoming of this model is it does not work in multiple-replica settings. In [50] keeping in view the problem of server collusion and no evidence on storage of multiple copies of data proposed multiple-replica PDP. The scheme empowers the client to store replicas of files with a challenge response protocol for verification. The MR-PDP scheme is better as compared to single-replica PDP scheme in computational aspect and can generate further replicas at lesser costs. The shortcoming of this scheme is it cannot perform public auditability.

In [51] used a model of indistinguishability obfuscation technique for remote data integrity auditing and reduced the computational burden of generation of signature for user. The model is useful in scenarios of outsourcing files by low-power client and verifications by cloud servers. In [52] proposed a model of protecting the privacy of the user to generate signatures by using third-party medium (TPM). The TPM is employed to develop a simple model for auditing integrity remotely. The TPM has an expiration time for authorization with a valid period. In [53], [54], [55] and in [56] Yu and Wang focused on reducing the damage of key exposure. They introduced remote auditing schemes which are key-exposure resilient and based on key update techniques in various scenarios.

Information sharing is an important aspect in cloud storage. In [57] keeping in view data sharing as a key aspect introduced a privacy-preserving approach that enables public auditing on cloud. The scheme focuses on modifying the ring signature for secured cloud storage. The scheme has the capacity to perform multiple auditing tasks at once. In [58] designed a public auditing scheme to store identity confidentiality for a group of members at once. The scheme uses blind signature technique for authentication.

In [59] proposed a privacy based public auditing method. The scheme is modeled for shared cloud data by generating a homomorphic verifiable group signature. The model needs a minimum of t group managers avoiding single-authority abuse and the users can track data changes in an assigned binary tree. In [60] keeping in view the risk of modification and sharing of data for a revoked user introduced an approach tailored for the shortcoming. It is a public auditing mechanism to ensure integrity where the cloud server re-signs data blocks of the revoked user. The scheme supports multiple auditing tasks verification at once. In [61] designed a scheme supporting user revocation in shared data integrity auditing. This scheme is designed to avoid compromise keeping in view the complacency between revoked users and malicious cloud servers. The scheme is tailored on secret sharing and polynomial-based authentication tags.

In [62] introduced identity-based proxy-oriented data uploading with remote integrity in public cloud (ID-PUIC). The system and security model are defined and ID-PUIC protocol is based on bilinear pairings. Further the ID-PUIC protocol is secure on hardness of CDH. In [63] introduced identity-based remote data integrity checking (RDIC) protocol. The scheme uses homomorphic cryptography. It reduces the costs for the management of PKI modeled RDIC protocols. In [64] the author

introduced incentive and unconditionally anonymous identity-based public PDP scheme. IAID-PDP system and security model are defined and the protocol is based on bilinear pairings. IAID-PDP is secure and eliminates the certificate management. In [65] introduced a scheme of user revocation without affecting the blocks held by the revoked user. Instead of focusing on the verifiers of the revoked user the model focused on updating the non-revoked group keys. The scheme is made on ID cryptography it does not need certificate management as needed in Public Key Infrastructure (PKI) systems. Further many other aspects were focused on such as privacy-preserving authentication in [66] and data deduplication [67] and [68] in remote data integrity auditing. Despite all these approaches the remote data integrity approaches mentioned above cannot completely support data sharing with information hiding.

In [69] based on earlier works developed an improvised model of PDP data checking remotely. The model focused on reducing the I/O costs by random sampling of blocks from the server. The challenge/response protocol reduces network communication making the model lightweight and more suitable for distributed storage scenarios. The authors presented two PDP schemes better than previous approaches. The shortcoming noticed was the model is not suitable for public audit.

In [70] Merkle introduced protocols for public key systems. The paper focused on unique properties and protocols on public keys and digital signatures along with comparisons. In [71] focused on a paper of cryptographic cloud storage. The paper focused on developing a secure cloud on a public cloud. Various architectures are described at a higher level and the benefits that accrue for customers and service providers. In [72] the author introduced a lesser energy-consuming protocol in the integrity of storage services on mobile cloud. The model focused on reducing mobile energy consumption while supporting dynamic operations. The authors used the concepts of incremental cryptography and trusted computing.

In [73]. proposed a mechanism of Message Authentication Code (MAC) for two parties communicating across an insecure channel. The model focused on authentication tag and shared key approach between two parties for data communication. In [74] introduced data access control for multi-authority cloud storage (DAC-MACS). The model is developed as new CP-ABE scheme. The key features are competent decryption and feature revocation for forward and backward security. In [75] investigated on [74] and proposed that there is a security vulnerability in the model where a revoked user can decode new ciphertexts based on an attack method revoke

In [76] the author proposed identity-based remote data possession checking (ID-RDPC) protocols. The protocol is secure assuming CDH. The key benefit of this approach is bypassing the process of certificate management. Further the model performs better as compared to RDPC protocols in PKI framework on: computation, communication and associated costs. In [77] constructed a protocol where they combined ID-based signature and public verification. This model enables the TPA to bypass the user task checking and focus purely on integrity of data. In [78] the author proposed a cancelable identity-based encryption (IBE) model that reduces the various tasks related to key management by enabling key update on cloud. This is done by introducing outsourcing computation into IBE to handle identity revocation. The model reduces the operational tasks for “Private Key Generator (PKG)” and users.

In [79] addressed the key management by proposing fuzzy identity-based auditing. In this model a user identity is a set of descriptive characteristics built as a protocol through biometrics. The protocol has been proven on CDH and discrete logarithm. In [80] the author addressed the issues of verifying public key certificates and their management. The author proposed “identity-based cloud data integrity checking protocol (ID-CDIC)”. The model proposed to eliminate certificate administration in out-of-date cloud checking.

Integrity verification in cloud storage is a topic of interest in recent times for researchers. In [81] introduced the concept of checking of files for integrity. They

based the model on challenge-response protocols and the challenge is generated randomly. The main shortcoming of this model was it is unsuitable for large amount of data load for verification. This is improvised by [1] with a scheme for PDP with RSA signatures. The RSA signatures had a drawback of tags of 1024 bits increasing costs and the scheme is incapable of privacy preserving if there is a TPA. Further [7] used BLS signatures over [1] RSA signatures limiting the length to 160 bits with security. In addition, work [8] on privacy-preserving public auditing for cloud joining HLA and random masking. In [82] proposed a signature scheme on CDH assumption. The secure signature length is 50% of DSA signature and suitable in cases of human typing or communicated simple bandwidth. In [83] proposed a public auditing scheme based on hash table dynamic in nature (DHT). It is a 2D structure present at a third parity auditor (TPA). The scheme reduces computational and communication aspects by transferring the information from the CSP to the TPA. The scheme a good updating efficiency, supports privacy preservation, enables batch auditing through BLS signatures. Over this [13] improvised the dynamic verification scheme with multiple owners.

In [84], [85] introduced a scheme with critical information hiding. It is a remote auditing scheme that uses a cleanser to mask critical information on the blocks while enabling remote integrity auditing. The scheme is based on ID cryptography. In [86] keeping in view multiple cloud service providers working in tandem proposed a cooperative PDP scheme. The scheme is based on homomorphic verifiable response and hash index and the model proved to have lesser cost and overhead aspects in comparison with non-cooperative approaches. This model resonates with [49] that focused on ID-DPDP. In [84] introduced ID multi replica PDP (IDPMR-PDP). The scheme provides TPA with multiple replicas without PKI. The scheme is protected against malicious servers and attackers. In [87] proposed a scheme named MuR-DPA that is an authenticated data structure (ADS) based on the MHT. The scheme enabled for the authentication of active datasets with multiple replicas on the cloud by including values in computation of MHT nodes in a top-down order as replica sub-tree. All the approaches for integrity verification are epoch-based auditing having time periods and the attacks can be detected at the completion of each period. Also, the ambiguity in the real verifier being the user or third-party, trusted and authorized is also a concern.

Motivated by integrity audit shortcomings some schemes comprising real-time assessment and fair mediation have been proposed. In [88] a scheme where checking is performed with each file used in operation. A data structure has been developed called FBH-Tree that stores the hash values. A file in operation requests a part which is the hash value for real time authentication. The scheme suffers from drawbacks in efficiency and computation overhead is directly proportional to incremental FBH-Tree. In [89] and in [90] proposed a similar kind of model where the motive to cheat is taken into account with party being either client or CSP. To overcome this, they introduce a third-party arbitrator based on signature exchange idea. The limitation to these models is that an exchange implies consent between parties with dispute resolution if arises is postponed to a later date.

For overcoming the problem of authentication reversible watermarking is a novel technique on which few models are discussed below. In [91] investigated high-capacity no loss data-embedding for images where the authentic image can be restored from the watermarked image. They presented two techniques (i) least significant bit prediction and Sweldens' lifting scheme (ii) improvement of Tian's technique of difference expansion. They also compared the techniques with various other embedding methods. In [92] proposed changeable image masking approach over encrypted field. In this model using an SVM classifier by decoder the distinction is made between encrypted and nonencrypted image patches and get the embedded message and original image. In [93] proposed reversible hiding scheme based on Shamir’s sharing. The information is distributed in random shares with the embedded information key shared to the correct owner. Using the key, the data can be extracted

either directly or by media authentication. In [94] proposed a changeable watermarking algorithm. In this method the authentic image is embedded with digital meta-data with removal at a later time. The loss less recovery of original image enables a digital signature of image to be embedded in the image itself only to be recovered later for authentication. In [95] presented a reversible hiding algorithm. After extracting the data, the authentic image is secured without disruption from the marked image. The algorithm alters the pixel values to implant the information in a histogram shifting modulation.

In [96] Tian proposed a DE modulation-based algorithm. The Difference Expansion algorithm capable to overcome overflow and underflow problems. This is achieved by calculation of the variance of adjacent pixel values to select some for DE to embed watermark. In [97] improvised in [95] skewed histogram shifting where the model uses a set of extreme predictions. By this the distortion problem is addressed in a better way by embedding the skewed structure histogram pixels from peak and short tail. In [98] used a method of lossless watermarking where parts of image are reversibly watermarked with message embedding by conventional Haar wavelet transform coefficients. The approach is one of the most competitive with high capacity and low distortion. In [99] experimented with identification of areas in an image considered most ideal for watermarking and embed the area by histogram shifting.

In [100] introduced a prediction error expansion (PEE) method. This model is derived from DE and Histogram Shifting (HS) approaches. The variance between the pixel and its estimate is used for data implanting. The models introduced also need to embed auxiliary information overhead.

In [101] Coltuc aimed at reduction in embedding distortion of prediction error. The method used here is not embedding the entire stretched difference but split the variance of current pixel and its calculation context. Testing is done on various changeable watermarking schemes. SGAP yielded the best results. In [102] pair wise prediction-error expansion (PEE). The sequence results in a 2D prediction-error histogram improves performance due to a better embedding approach. In [103] improvised on [102] and proposed a familiar kind of pixel pairing. In this approach only pixels with similar prediction errors are paired and embedded thereby decreasing the number of shifted pixels. In [104] introduced a segmented data embedding method for efficient RDH. In this method the host is not considered as a whole but partitioned into multiple sub hosts. Each sub host can have its own embedding enabling to apply varied RDH algorithms as an ensemble. The major shortcomings in all the schemes of reversible watermarking are to provide stable capacity and exposure of images to be checked.

3 Conclusion

This review paper explores the most ideas of data integrity and security problems in the distributed cloud computing environment along with some models, challenges, and limitations involved in this field. IT presented many of the data security concepts on cloud servers such as, schemes, protocols, algorithms, access policies, storage scenarios, access services, and a third-party auditor.

A comparison for eight models of data integrity and security models was done based on common six features, public auditing, privacy preserving, data dynamic, batch auditing, data integrity, data confidentiality. Besides the two models, homomorphic tokens with erasure code and HMAC algorithm, several enhanced models of HLA and MHT combinations were compared too. HLA and MHT used with a diversity of schemes and algorithms, HLA used with random masking, BLS signature, BLS signature along with MHT, and AES algorithm. Whereas MHT is used individually and/or combined either with BLS signature, or with RSA algorithm.

The three security features, public auditing, privacy preserving, and data integrity were satisfied by all models. Both, data dynamics and batch auditing integrity, were satisfied by three models. Whereas data confidentiality was satisfied in two models only. Two models of data integrity and security, HLA with random masking and AES algorithm, HLA with BLS signature along with MHT, satisfied (83%) of the required features. All features except data confidentiality and data dynamic. Four models satisfied with (66.6%), and two models satisfied with only (33%) of the features.

This review investigated a lack of data integrity and security models with certain required features like data confidentiality, data dynamics and batch auditing integrity. The work on data confidentiality and data dynamics of the cloud security can be extended by adding these features in different models. So, more research can be done to improve HLA with random masking, and HMAC Algorithm models by adding more features of data integrity and security.

Studying possibilities of adding advanced security features for models such as, HLA with BLS signature, MHT and RSA algorithm, and HMAC Algorithm, can be investigated in future research.

References

1. G. Ateniese, R. Burns, R. Curtmola, et al. Provable data possession at untrusted stored [C]//Proc of the 14th ACM Conference on Computer and Communications Security. New York: ACM, 2007: 598-609.
2. M.A. Shah, M. Baker, J.C. Mogul, R. Swaminathan, "Auditing to keep online storage services honest," In: HOTOS'07: Proceedings of the 11th USENIX Workshop on Hot Topics in Operating Systems, Berkeley, CA, USA, pp. 1–6 (2007).
3. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, pp. 213–222, (2009).
4. Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," IEEE Trans. Knowl. Data Eng., vol. 23, no. 9, pp. 1432–1437, (2011)
5. A.F. Barsoum, M.A. Hasan, "On verifying dynamic multiple data copies over cloud servers," In: Cryptology ePrint Archive, Report 2011/447. http://eprint.iacr.org/ (2011).
6. A. Juels and B. S. K. Jr, "Pors: Proofs of retrievability for large files," in Proceedings of CCS. ACM, 2007, pp. 583–597.
7. H. Shacham and B. Waters, "Compact proofs of retrievability," in Proceedings of ASIACRYPT. Springer, 2008, pp. 90–107.
8. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.
9. Y. Zhang, C. Xu, S. Yu, H. Li, and X. Zhang, "Sclpv: Secure certificateless public verification for cloud-based cyber-physical-social systems against malicious auditors," IEEE Transactions on Computational Social Systems, vol. 2, no. 4, pp. 159–170, 2015.
10. M. Sookhak, A. Gani, H. Talebian, A. Akhunzada, S. U. Khan, R. Buyya, and A. Y. Zomaya, "Remote data auditing in cloud computing environments: A survey, taxonomy, and open issues," ACM Computing Surveys, vol. 47, no. 4, 2015.
11. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of SecureComm. ACM, 2008.
12. E. Shi, E. Stefanov, and C. Papamanthou, "Practical dynamic proofs of retrievability," in Proceedings of CCS. ACM, 2013, pp. 325–336.
13. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717–1726, 2013.
14. M. Sookhak, A. Gani, M. K. Khan, and R. Buyya, "Dynamic remote data auditing for securing big data storage in cloud computing," to appear, doi: 10.1016/j.ins.2015.09.004.
15. Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. In INFOCOM, 2010 Proceedings IEEE, pages 1–9. IEEE, 2010.

16. Cong Wang, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy Preserving Public Auditing for Secure Cloud Storage. http://eprint.iacr.org/2009/579.pdf
17. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li. Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. Parallel and Distributed Systems, IEEE Transactions on, 22(5):847–859, 2011.
18. Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou. Toward secure and dependable storage services in cloud computing. Services Computing, IEEE Transactions on, 5(2):220–232, 2012.
19. Solomon GuadieWorku, Chunxiang Xu, Jining Zhao, and Xiaohu He. Secure and efficient privacy-preserving public auditing scheme for cloud storage. Computers & Electrical Engineering, 40(5):1703–1713, 2014.
20. IK Meenakshi and Sudha George. Cloud Server Storage Security using TPA. International Journal of Advanced Research inComputer Science & Technology (IJARCST) ISSN: 2347-9817, 2014.
21. Tejaswini, K. Sunitha, and S. K. Prashanth. Privacy Preserving and Public Auditing Service for Data Storage in Cloud Computing. Indian Journal of Research PARIPEX, 2(2), 2013.
22. Jadhav Santosh and B.R nandwalkar. Privacy Preserving and Batch auditing in Secure Cloud Data Storage using AES. Proceedings of 13th IRF International Conference, ISBN: 978-93-84209-37-72014.
23. S Ezhil Arasu, B Gowri, and S Ananthi. Privacy-Preserving Public Auditing in cloud using HMAC Algorithm. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277, 3878, 2013.
24. Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou. “Towards Secure and Dependable Storage Services in Cloud Computing”. IEEE Transactions on Services Computing, Volume 5, Issue 2, pp. 220–232, May 2011.
25. Swapnali Morea, Sangita Chaudhari , “Third Party Public Auditing Scheme for Cloud Storage”, International Journal of Procedia Computer Science, Volume 79, pp. 69-76, 2016.
26. S. Berger, S. Garion, Y. Moatti, D. Naor, D. Pendarakis, A. ShulmanPeleg, J. R. Rao, E. Valdez, and Y. Weinsberg, “Security intelligence for cloud management infrastructures,” IBM Journal of Research and Development, vol. 60, no. 4, pp. 11:1–11:13, 2016.
27. Secure access control for cloud storage,” https://www.research.ibm. com/haifa/projects/storage/cloudstorage/secure access.shtml.
28. D. Boneh, C. Gentry, and B. Waters, “Collusion resistant broadcast encryption with short ciphertexts and private keys,” in CRYPTO 2005, ser. LNCS, vol. 3621, 2005, pp. 258–275.
29. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1–30, 2006.
30. L. Zhou, V. Varadharajan, and M. Hitchens, “Achieving secure rolebased access control on encrypted data in cloud storage,” IEEE Trans. Information Forensics and Security, vol. 8, no. 12, pp. 1947–1960, 2013.
31. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, 2006, pp. 89–98.
32. V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, “Attribute-based access control,” IEEE Computer, vol. 48, no. 2, pp. 85–88, 2015.
33. N. Attrapadung, B. Libert, and E. de Panafieu, “Expressive key-policy attribute-based encryption with constant-size ciphertexts,” in PKC 2011, ser. LNCS, vol. 6571, 2011, pp. 90–108.
34. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in 2007 IEEE Symposium on Security and Privacy (S&P 2007), 2007, pp. 321–334.
35. B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in PKC 2011, ser. LNCS, vol. 6571, 2011, pp. 53–70.
36. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in INFOCOM 2010, 2010, pp. 534–542.
37. J. Huang, C. Chiang, and I. Liao, “An efficient attribute-based encryption and access control scheme for cloud storage environment,” in Grid and Pervasive Computing GPC 2013, ser. LNCS, vol. 7861, 2013, pp. 453– 463.
38. G. Wang, Q. Liu, and J. Wu, “Hierarchical attribute-based encryption for fine-grained access control in cloud storage services,” in Proceedings of the 17th ACM Conference on

Computer and Communications Security, CCS 2010, 2010, pp. 735–737.

39. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, 2013.
40. Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 743– 754, 2012.
41. Y. Wu, Z. Wei, and R. H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing networks," IEEE Trans. Multimedia, vol. 15, no. 4, pp. 778–788, 2013.
42. J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282, 2013.
43. A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in CRYPTO 2012, ser. LNCS, vol. 7417, 2012, pp. 199–217.
44. K. Yang, X. Jia, and K. Ren, "Secure and verifiable policy update outsourcing for big data access control in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 12, pp. 3461–3470, 2015.
45. K. Liang, L. Fang, D. S. Wong, and W. Susilo, "A ciphertext-policy attribute-based proxy re-encryption scheme for data sharing in public clouds," Concurrency and Computation: Practice and Experience, vol. 27, no. 8, pp. 2004–2027, 2015.
46. G. Yang, C. H. Tan, Q. Huang, and D. S. Wong, "Probabilistic public key encryption with equality test," in Topics in Cryptology - CT-RSA 2010, ser. LNCS, vol. 5985, 2010, pp. 119–131.
47. Q. Tang, "Towards public key encryption scheme supporting equality test with fine-grained authorization," in Information Security and Privacy - 16th Australasian Conference, ACISP 2011, ser. LNCS, vol. 6812, 2011, pp. 389–406.
48. Tang, Qiang. Public key encryption schemes supporting equality test with authorisation of different granularity," IJACT, vol. 2, no. 4, pp. 304– 321, 2012.
49. Wang H. Identity-Based Distributed Provable Data Possession in Multicloud Storage[J]. IEEE Transactions on Services Computing, 2015, 8(2):328-340.
50. Curtmola R, Khan O, Burns R, et al. MR-PDP: Multiple-Replica Provable Data Possession[C]// The, International Conference on Distributed Computing Systems. IEEE Computer Society, 2008:411-420.
51. C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, "Symmetrickey based proofs of retrievability supporting public verification," in Computer Security—ESORICS. Cham, Switzerland: Springer, 2015, pp. 203–223.
52. W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium," J. Netw. Comput. Appl., vol. 82, pp. 56–64, Mar. 2017.
53. J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1167–1179, Jun. 2015.
54. J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1362–1375, Jun. 2016.
55. J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1931–1940, Aug. 2017.
56. J. Yu, R. Hao, H. Xia, H. Zhang, X. Cheng, and F. Kong, "Intrusionresilient identity-based signatures: Concrete scheme in the standard model and generic construction," Inf. Sci., vols. 442–443, pp. 158–172, May 2018.
57. B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in Proc. IEEE 5th Int. Conf. Cloud Comput. (CLOUD), Jun. 2012, pp. 295–302.
58. G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," J. Syst. Softw., vol. 113, pp. 130–139, Mar. 2016.
59. A. Fu, S. Yu, Y. Zhang, H. Wang, and C. Huang, "NPP: A new privacy-aware public auditing scheme for cloud data sharing with group users," IEEE Trans. Big Data, to be published, doi: 10.1109/TBDATA.2017.2701347.
60. B. Wang, B. Li, and H. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Trans. Serv. Comput., vol. 8, no. 1, pp. 92–106, Jan./Feb. 2015.

61. Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, “Efficient integrity auditing for shared data in the cloud with secure user revocation,” in Proc. IEEE Trustcom/BigDataSE/ISPA, Aug. 2015, pp. 434–442.
62. H. Wang, D. He, and S. Tang, “Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1165–1176, Jun. 2016.
63. Y. Yu et al., “Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage,” IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 767–778, Apr. 2017.
64. H. Wang, D. He, J. Yu, and Z. Wang, “Incentive and unconditionally anonymous identity-based public provable data possession,” IEEE Trans. Serv. Comput., to be published, doi: 10.1109/TSC.2016.2633260.
65. Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren, “Enabling efficient user revocation in identity-based cloud storage auditing for shared big data,” IEEE Trans. Depend. Sec. Comput., to be published, doi: 10.1109/TDSC.2018.2829880.
66. W. Shen, G. Yang, J. Yu, H. Zhang, F. Kong, and R. Hao, “Remote data possession checking with privacy-preserving authenticators for cloud storage,” Future Gener. Comput. Syst., vol. 76, pp. 136–145, Nov. 2017.
67. J. Li, J. Li, D. Xie, and Z. Cai, “Secure auditing and deduplicating data in cloud,” IEEE Trans. Comput., vol. 65, no. 8, pp. 2386–2396, Aug. 2016.
68. J. Hur, D. Koo, Y. Shin, and K. Kang, “Secure data deduplication with dynamic ownership management in cloud storage,” IEEE Trans. Knowl. Data Eng., vol. 28, no. 11, pp. 3113–3125, Nov. 2016.
69. Ateniese G., Burns R., Curtmola R.: Remote data checking using provable data possession. Acm Transactions on Information & System Security 14(1), 12-12 (2011).
70. Merkle R C.: Protocols for Public Key Cryptosystems. IEEE Symposium on Security & Privacy (3), 122-122 (1980).
71. Kamara S., Lauter K.: Cryptographic cloud storage. In: International Conference on Financial Cryptograpy and Data Security. Springer-Verlag, pp.136-149 (2010).
72. Itani W, Kayssi A, Chehab A.: Energy-efficient incremental integrity for securing storage in mobile cloud computing. In: International Conference on Energy Aware Computing. pp.1-2. IEEE, Cairo (2010).
73. Bellare M, Ran C, Krawczyk H.: Message Authentication using Hash Functions--- The HMAC Construction. Cryptobytes, 2 (1996,).
74. Yang K, Jia X, Ren K: DAC-MACS: Effective data access control for multi-authority cloud storage systems. In: INFOCOM, 2013 Proceedings IEEE. pp. 2895-2903. IEEE, Turin (2013).
75. Hong J., Xue K., Li W.: Comments on “DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems”/Security Analysis of Attribute Revocation in Multiauthority Data Access Control for Cloud Storage Systems. IEEE Transactions on Information Forensics & Security 10(6),1315-1317 (2017).
76. H. Wang, J. Domingo-Ferrer, Q. Wu, and B. Qin: Identity-based remote data possession checking in public clouds. IET Information Security 8(2), pp. 114–121 (2014).
77. Tan S., Jia Y.: NaEPASC: a novel and efficient public auditing scheme for cloud data. Frontiers of Information Technology & Electronic Engineering 15(9), 794-804 (2014).
78. Li J., Li J., Chen X.: Identity-Based Encryption with Outsourced Revocation in Cloud Computing. IEEE Transactions on Computers 64(2) 425-437 (2015).
79. Li Y., Yu Y., Min G.: Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems. IEEE Transactions on Dependable & Secure Computing, pp. (99):1-1 (2017).
80. Yu, Y., Xue, L., Man, H. A., Susilo, W., Ni, J., & Zhang, Y., et al.: Cloud data integrity checking with an identity-based auditing mechanism from RSA. Future Generation Computer Systems 62(C), 85-91 (2016).
81. Y. Deswarte, J. J. Quisquater, and A. Saïdane, ‘‘Remote Integrity Checking,’’ in Proc. 5th Work. Conf. Integrity Intl Control Inf. Syst. (IICIS), 2004, pp. 1–11.
82. D. Boneh, B. Lynn, and H. Shacham, ‘‘Short signatures from the weil pairing,’’ J. Cryptol., vol. 17, no. 4, pp. 297–319, 2004.
83. H. Tian et al., ‘‘Dynamic-hash-table based public auditing for secure cloud storage,’’ IEEE Trans. Service Comput., vol. 10, no. 5, pp. 701–714, Sep./Oct. 2017
84. S. Peng, F. Zhou, Q. Wang, Z. Xu, and J. Xu, ‘‘Identity-based Public Multi-Replica Provable Data Possession,’’ IEEE Access, vol. 5, pp. 26990–27001, 2017.
85. W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, ‘‘Enabling identity-based integrity auditing and

data sharing with sensitive information hiding for secure cloud storage,'' IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 331–346, Feb. 2019.
86. Y. Zhu, H. X. Hu, G.-J. Ahn, and M. Yu, ''Cooperative provable data possession for integrity verification in multicloud storage,'' IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231–2244, Dec. 2012.
87. C. Liu, R. Ranjan, C. Yang, X. Zhang, L. Wang, and J. Chen, ''MuRDPA: Top-down levelled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud,'' IEEE Trans. Comput., vol. 64, no. 9, pp. 2609–2622, Sep. 2015.
88. G.-H. Hwang and H.-F. Chen, ''Efficient real-time auditing and proof of violation for cloud storage systems,'' in Proc. IEEE 9th Intl Conf. Cloud Comput. (CLOUD), Jun./Jul. 2016, pp. 132–139.
89. H. Jin, H. Jiang, and K. Zhou, ''Dynamic and public auditing with fair arbitration for cloud data,'' IEEE Trans. Cloud Comput., vol. 6, no. 3, pp. 680–693, Jul./Sep. 2018.
90. A. Küpçü, ''Official arbitration with secure cloud storage application,'' Comput. J., vol. 58, no. 4, pp. 831–852, 2015.
91. L. Kamstra and H. J. A. M. Heijmans, ''Reversible data embedding into images using wavelet techniques and sorting,'' IEEE Trans. Image Process., vol. 14, no. 12, pp. 2082–2090, Dec. 2005.
92. J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au, and Y. Y. Tang, ''Secure reversible image data hiding over encrypted domain via key modulation,'' IEEE Trans. Circuits Syst. Video Technol., vol. 26, no. 3, pp. 441–452, Mar. 2016.
93. P. Singh and B. Raman, ''Reversible data hiding based on Shamir's secret sharing for color images over cloud,'' Inf. Sci., vol. 422, pp. 77–97, Jan. 2018.
94. C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, ''Lossless recovery of an original image containing embedded data,'' U.S. Patent 6 278 791 B1, Aug. 21, 2001.
95. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, ''Reversible data hiding,'' IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.
96. J. Tian, ''Reversible data embedding using a difference expansion,'' IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
97. S. Kim, X. Qu, V. Sachnev, and H. J. Kim, ''Skewed histogram shifting for reversible data hiding using a pair of extreme predictions,'' IEEE Trans. Circuits Syst. Video Technol., to be published. doi: 10.1109/TCSVT. 2018.2878932.
98. W. Pan, G. Coatrieux, N. Cuppens, F. Cuppens, and C. Roux, ''An additive and lossless watermarking method based on invariant image approximation and Haar wavelet transform,'' in Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. (EMBC), Aug./Sep. 2010, pp. 4740–4743.
99. G. Coatrieux, W. Pan, N. Cuppens-Boulahia, F. Cuppens, and C. Roux, ''Reversible watermarking based on invariant image classification and dynamic histogram shifting,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 111–120, Jan. 2013.
100. D. M. Thodi and J. J. Rodriguez, ''Expansion embedding techniques for reversible watermarking,'' IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.
101. D. Coltuc, ''Improved embedding for prediction-based reversible watermarking,'' IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 873–882, Sep. 2011.
102. B. Ou, X. Li, Y. Zhao, R. Ni, and Y.-Q. Shi, ''Pairwise prediction-error expansion for efficient reversible data hiding,'' IEEE Trans. Image Process., vol. 22, no. 12, pp. 5010–5021, Dec. 2013.
103. I.-C. Dragoi and D. Coltuc, ''Adaptive pairing reversible watermarking,'' IEEE Trans. Image Process., vol. 25, no. 5, pp. 2420–2422, May 2016.
104. H. Z. Wu, W. Wang, J. Dong, and H. X. Wang, ''Ensemble reversible data hiding,'' in Proc. 24th Int. Conf. Pattern Recognit. (ICPR), Aug. 2018, pp. 1–6.