AUDITING OF CLOUD STORAGE

R. Jothilakshmi
Associate Professor, Department of Information Technology, RMD Engineering college, Chennai, India.

Yadhindra Sri Varshan P A,Sudarshan R, Kireeti Adluru , UG student,Department of Information Technology,RMD Engineering college,Chennai,India

ABSTRACT

Cloud storage security has gained sizable analysis efforts with the wide adoption of cloud computing. As a security mechanism, researchers are investigating cloud storage auditing schemes that modify a user to verify whether or not the cloud keeps the user's outsourced information uninjured. However, existing schemes have usability problems in compatibility with existing world cloud storage applications, error-tolerance, and potency. To mitigate this usability gap, this paper proposes a brand new general cloud storage auditing theme that's a lot of usable. The projected theme uses the concept of group action linear error correcting codes and linear homomorphic authentication schemes along. This integration uses only 1 further block to attain error tolerance and authentication at the same time.

To demonstrate the facility of the overall construction, we have a tendency to conjointly propose one elaborated theme supported the projected general construction exploitation the Reed Solomon code and also the universal hash based mostly mack authentication theme, each of that square measure enforced over the computation-efficient Evariste Galois field GF(28). we have a tendency to conjointly show that the projected theme is secure underneath the quality definition. Moreover, we have a tendency to enforce and open-source the projected theme. Experimental results show that the projected theme is orders of magnitude more economical than the progressive theme.

1.INTRODUCTION

With each event of computers and Cloud computing technology,in recent years is to source data storage and process on Cloud-based services. The Cloud-based services for individual finish users are a unit gaining quality particularly for information storage. Looking forward to giant cupboard space and reliable communication channels, Cloud-based service suppliers like Dropbox, Google Drive, or Amazon Drive simply call many area units providing individual users with virtually infinite and inexpensive cupboard space. This situation raises the question of the trait of Cloud service suppliers. several information security and privacy incidents area units determined in today’s Cloud services. On the one hand, Cloud service suppliers take care of an outsized range of external attacks. In 2018, a complete of one.5 million Sing Health patients’ non-medical personal information were purloined from the health system in Singapore. On the opposite hand, Cloud service suppliers can not be entirely trusty either. Personal information is also exploited in an exceedingly malicious method like within the Facebook and Cambridge Analytical information scandal that affected eighty seven million users in 2018. Thus, it becomes progressively necessary for finished users to expeditiously defend their information (texts, images, or videos) severally from Cloud service suppliers. One cheap answer is to shield information on a secure finish user’s waterproof hine before outsourcing to Clouds that naturally becomes ancient ciphers like AES. However, coding algorithms area unit transferring protection on information to protection on keys that successively, introduces key management issues. Once the secret is exposed, information security is going to be vulnerable. Worse, if the top users don't have any cryptography smart follow and take a look at to utilize an equivalent key for various information protection; one key exposure can result in a large vary of information run. Thus, additionally to ciphers, different information protection schemes are a unit necessary to support such situations**.**

2.LITERATURE SURVEY

TITLE**:** Privacy-preserving public auditing for shared cloud data supporting group dynamics

AUTHOR: B. Wang, H. Li and M. Li

YEAR: 2013

DESCRIPTION:

In the cloud, data is often shared by a group of users. To ensure the long-term correctness of cloud shared data, a third-party public verifier can be introduced to audit data integrity. During the auditing, protecting the privacy of the contributors of shared data from the public auditor is a fundamental issue. However, this makes it challenging to simultaneously support group membership dynamics efficiently, due to the significant amount of computation needed to update the signatures on shared data. In this paper, we propose a novel privacy-preserving public auditing mechanism for shared cloud data. With our proposed mechanism, a public verifier is able to audit the integrity of shared data without retrieving the entire data from the cloud, and also without learning private identity information of the group members. Group dynamics (user join and user revocation) are efficiently handled by outsourcing signature updating operations to the cloud via a secure proxy re-signature scheme. Experimental results show that our mechanism is highly efficient for dynamic groups . 3 In the cloud, data is often shared by a group of users. To ensure the long correctness of cloud shared data, a third-party public verifier can be introduced to audit data integrity. During the auditing, protecting the privacy of the contributors of shared data from the public auditor is a fundamental issue. However, this makes it challenging to simultaneously support group membership dynamics efficiently,due to the significant amount of computation needed to update the signatures on shared data.In this paper,we propose a novel privacy-preserving public auditing mechanism for shared cloud data With our proposed mechanism, a public verifier is able to audit the integrity of shared without retrieving the entire data from the cloud, and also without learning private id. information of the group members

TITLE**:** A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability

AUTHOR**:** Z. Hao, S. Zhong and N. Yu

YEAR: 2011

DESCRIPTION

Remote data integrity checking is a crucial technology in cloud computing. Recently, many works focus on providing data dynamics and/or public verifiability to this type of protocol. Existing protocols can support both features with the help of a third-party auditor. In a previous work, Sebé et al. propose a remote data integrity checking protocol that supports data dynamics. In this paper, we adapt Sebé et al.'s protocol to support public verifiability. The proposed protocol supports public verifiability without help of a third-party auditor. In addition , the proposed protocol does not leak any private information to third-party verifiers. Through a formal analysis, we show the correctness and security of the protocol. After that, through theoretical analysis and experimental results, we demonstrate that the proposed protocol has a good performance**.**

TITLE: Toward Efficient Multi-Keyword Fuzzy Search Over Encrypted Outsourced Data With Accuracy Improvement

AUTHOR: Z. Fu, X. Wu, C. Guan, X. Sun and K. Ren

YEAR: 2016

DESCRIPTION

Keyword-based search over encrypted outsourced information has become a vital tool in the current cloud computing situation. The bulk of the present techniques square measure focusi metric weight unit on multi-keyword actual match or single keyword fuzzy search. However, those existing techniques find less sensible significance in real-world applications compared with the multi-keyword 4fuzzy search technique over encrypted information. the primary plan to construct such a multi -keyword fuzzy search theme was reportable by Wang et al., United Nations agency used locality-sensitive hashing functions and Bloom filtering to satisfy the goal of multi-keyword fuzzy search. still, Wang's scheme was solely effective for a 1 letter mistake in keyword however wasn't effective for different common writing system mistakes. Moreover, Wang's theme was at risk of server out-of-order problems throughout the ranking method and failed to contemplate the keyword weight. during this p human, based on Wang et al.'s scheme, we tend to propose AN economical multi-keyword fuzzy stratified search scheme supported Wang et al.'s theme that's able to address the aforesaid problems. First, We develop a brand new methodology of keyword transformation supported by the uni-gram, which will simultaneously improve the accuracy and create the power to handle different writing system mistakes.

In Addition, keywords with a similar root will be queried for exploitation of the algorithmic program.

Furthermore, we tend to contemplate the keyword weight once choosing AN adequate matching file set . Experiments exploitation real-world information show that our theme is much economical and achieve high accuracy.

III.PROPOSED SYSTEM

In the context of cloud computing, sticky policies are planned to precise needs on the protection and geographical location of storage nodes. However, to date it's been unclear however this might be complete with efficiency in an exceedingly massive and distributed storage system. With PRADA, we tend to give a mechanism to attain this goal.

The possible load balance depends on how well the nodes' capabilities to meet bound DHRs match the particular DHRs requested by the purchasers. However, for a given situation, PRADA is in a position to attain nearly best load balance; the planned approaches like audit work, data flow management, and obvious knowledge possession may also be applied to PRADA.

Homomorphic Algorithm

Homomorphic encryption is a form of encryption allowing one to perform calculations on encrypted data without decrypting it first. The result of the computation is in an encrypted form, when decrypted the output is the same as if the operations had been performed on the unencrypted data.

1. Choose two large prime numbers p and q randomly and independently of each other such that gcd(pq,(p-1)(q-1))=1. This property is assured if both primes are of equal length.

2. Compute n=pq and lambda =lcm(p-1,q-1)

3. Select random integer g where g ε $□^{*}_{□}$2.

4. Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse : □=(L(g mod n)) mod n lambda 2 −1 where function L divides as L(x)= n x−1.

5. Note that the notation does not denote the modular multiplication of b a a times the modular multiplication of a times the modular multiplicative inverse of b but rather the quotient of a divided by b.

The Public Key (encryption key) is (n,g).

The Private Key (decryption key) is (, lambda □)

Encryption:

1. Let m be a message to be encrypted where 0 m<n. ≤

2. Select random r where 0 r<n

3. Compute Cipher text as c=$□^{□}$. $□^{□}$ mod $□^{2}$

Decryption:

1. Let c be the cipher text to decrypt c εZ* n 2

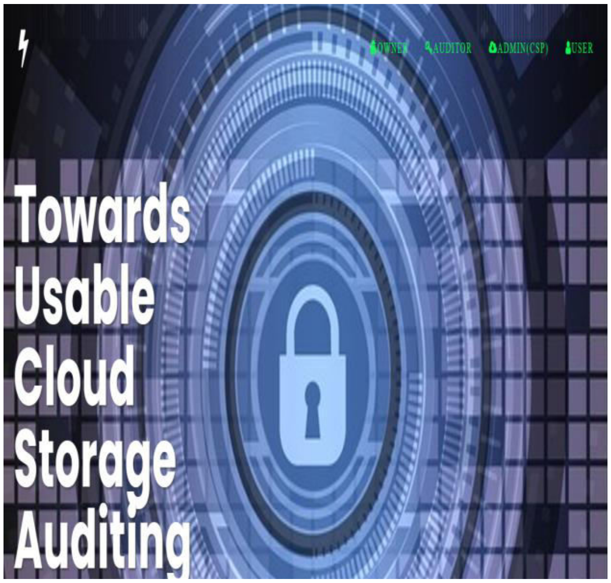
2. Compute the plaintext message m= L(c mod n). Mu mod n.

IV.RESULTS AND DISCUSSIONS

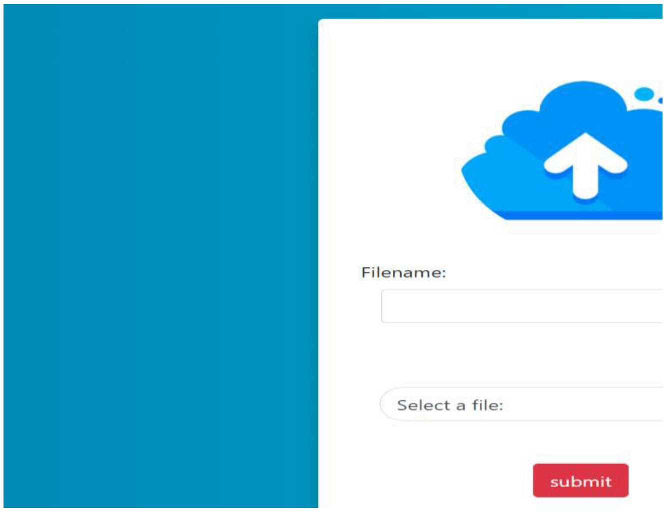
1. OWNER

1.Initially if the owner is new to cloud , then owner can register else Owner can login and view the owner account.

2.Owner can upload any file which the owner prefers (i.e) .txt,.pdf etc. 3.Owner can also have the access to view the details of the user's login.



HOMEPAGE



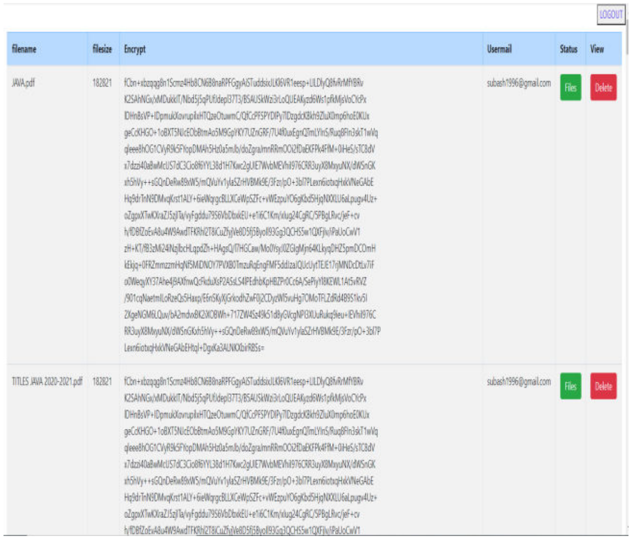
FILE UPLOAD

2) **Auditor**

1. As there is only one Auditor, Auditor can directly login with Auditor credentials

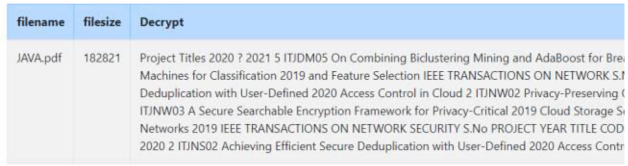
2. Now the Auditor can audit the files.

3. Here the content of files is encrypted and while clicking the files button, Decrypted content of the file will be present and it is the actual content which is being uploaded by the owner. Based on the content, the auditor accepts or rejects it.



filename	filesize	Encrypt	Usermail	Status	View
JAVA.pdf	182821	fCbn+xbzqqg8n1Scmz4Hb8CN6B8naRPFGgyAiSTuddsixJLKI6VR1eesp+LILDlyQ8fvRrMfYBRv K2SAhNGx/xMDukkIT/Nbd5j5qPUfJdepl37T3/B5AUSkWzi3rLoQUEAKyzd6Ws1pfkMjsVoCYcPx lDHn8sVP+lDpmukXovrupIxHTQzeOtuwmC/QfCcPFSPYDlPy7lDzgdcK8kh9ZluX0mp6hoE0KUx geCcKHGO+1oBXT5NJcEObBtmAo5M9GpYKY7UZnGRF/7U4f0uxEgnQTmLYlnS/Ruq8Fln3skT1wVq qleee8hOG1CVyR9k5FYopDMAh5Hz0a5mJb/doZgraJmnRRmOOi2fDaEKFPk4FfM+0iHeS/sTC8dV x7dzzi40aBwMcUS7dC3Cio8f6YYL38d1H7Kwc2gUIE7WvbMEVhil976CRR3uyX8MxyuNX/dWSnGK xh5hVy++sGQnDeRw89xW5/mQVuYv1ylaSZrHVBMk9E/3Fzr/pO+3bl7PLexn6iotxqHxkVNeGAbE Hq9drTnN9DMvqKrst1ALY+6ieWqrgcBLLXCeWpSZFc+vWEzpuYO6gKbd5HjqNXXLU6aLpugv4Uz+ oZgpxXTwKXraZJ5zjlTa/vyFgddu79S6VbDbxkEU+e1i6C1Km/xlug24CgRC/5PBgLRvc/jeF+cv h/fDBfZoEvA8u4W9AwdTFKRhl2T8iCuZfyjVe8D5fj5ByoII93Gg3QCHS5w1QXFjlv/iPaUoCwV1 zH+KT/fB3zMi24lNzjlbcHLqpdZh+HAgsQ/lTHGCaw/Mo0YsyI0ZGlgMjn64KLkyqDHZ5pmDCOmH kEkjq+0FRZmmzzmHqNf5MiDNOY7PVXB0TmzuRqEngfMF5ddIzaJQUcUytTEJE17rjMNDcDtLv7iF o0WeqyXY37Ahe4jBAXfnwQcFkduXsP2ASsLS4lPEdhbKpHBZPr0Cc6A/SePlyYI8KEWL1At5vRVZ /901cqNaetmlLoRzeQs5Haxp/E6nSKyXjGrkodhZwF0j2CDyzW15vuHg7OMoTFLZdRd4B9S1kv5I 2XgeNGM6LQuv/bA2mdvxBK2iXOBWh+717ZW4Sz49k51d8yGVcgNPI3XUuRukq9ieu+lEVhil976C RR3uyX8MxyuNX/dWSnGKxh5hVy++sGQnDeRw89xW5/mQVuYv1ylaSZrHVBMk9E/3Fzr/pO+3bl7P Lexn6iotxqHxkVNeGAbEHtql+DgxKa3ALNKXbirRB5s=	subash1996@gmail.com	Files	Delete
TITLES JAVA 2020-2021.pdf	182821	fCbn+xbzqqg8n1Scmz4Hb8CN6B8naRPFGgyAiSTuddsixJLKI6VR1eesp+LILDlyQ8fvRrMfYBRv K2SAhNGx/xMDukkIT/Nbd5j5qPUfJdepl37T3/B5AUSkWzi3rLoQUEAKyzd6Ws1pfkMjsVoCYcPx lDHn8sVP+lDpmukXovrupIxHTQzeOtuwmC/QfCcPFSPYDlPy7lDzgdcK8kh9ZluX0mp6hoE0KUx geCcKHGO+1oBXT5NJcEObBtmAo5M9GpYKY7UZnGRF/7U4f0uxEgnQTmLYlnS/Ruq8Fln3skT1wVq qleee8hOG1CVyR9k5FYopDMAh5Hz0a5mJb/doZgraJmnRRmOOi2fDaEKFPk4FfM+0iHeS/sTC8dV x7dzzi40aBwMcUS7dC3Cio8f6YYL38d1H7Kwc2gUIE7WvbMEVhil976CRR3uyX8MxyuNX/dWSnGK xh5hVy++sGQnDeRw89xW5/mQVuYv1ylaSZrHVBMk9E/3Fzr/pO+3bl7PLexn6iotxqHxkVNeGAbE Hq9drTnN9DMvqKrst1ALY+6ieWqrgcBLLXCeWpSZFc+vWEzpuYO6gKbd5HjqNXXLU6aLpugv4Uz+ oZgpxXTwKXraZJ5zjlTa/vyFgddu79S6VbDbxkEU+e1i6C1Km/xlug24CgRC/5PBgLRvc/jeF+cv h/fDBfZoEvA8u4W9AwdTFKRhl2T8iCuZfyjVe8D5fj5ByoII93Gg3QCHS5w1QXFjlv/iPaUoCwV1	subash1996@gmail.com	Files	Delete

File Content view and Encryption



filename	filesize	Decrypt
JAVA.pdf	182821	Project Titles 2020 ? 2021 5 ITJDM05 On Combining Biclustering Mining and AdaBoost for Brea Machines for Classification 2019 and Feature Selection IEEE TRANSACTIONS ON NETWORK S.N Deduplication with User-Defined 2020 Access Control in Cloud 2 ITJNW02 Privacy-Preserving C ITJNW03 A Secure Searchable Encryption Framework for Privacy-Critical 2019 Cloud Storage Se Networks 2019 IEEE TRANSACTIONS ON NETWORK SECURITY S.No PROJECT YEAR TITLE COD 2020 2 ITJNS02 Achieving Efficient Secure Deduplication with User-Defined 2020 Access Contr

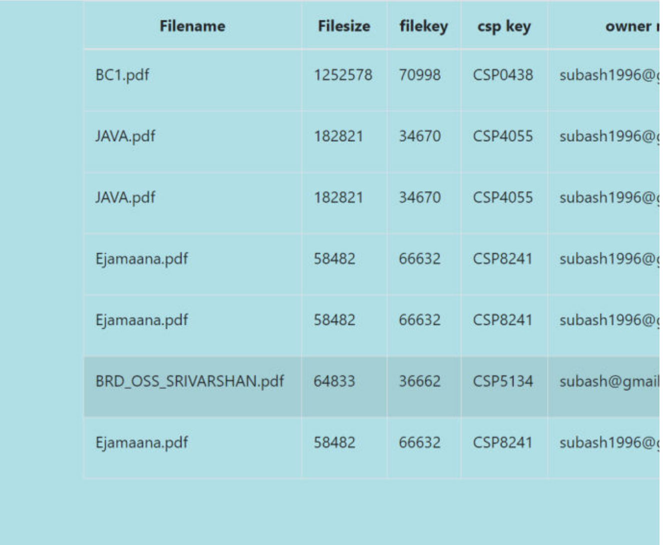
File Content view and Decryption

3. Admin

1. Similar to an auditor, there will be only one admin . Admin can login with admin credential.

2. Admin can also view the user's login.

3. Now the admin is responsible for sending the key which is required by the user to download. Once after a user request , the admin can send the key .



Filename	Filesize	filekey	csp key	owner
BC1.pdf	1252578	70998	CSP0438	subash1996@g
JAVA.pdf	182821	34670	CSP4055	subash1996@g
JAVA.pdf	182821	34670	CSP4055	subash1996@g
Ejamaana.pdf	58482	66632	CSP8241	subash1996@g
Ejamaana.pdf	58482	66632	CSP8241	subash1996@g
BRD_OSS_SRIVARSHAN.pdf	64833	36662	CSP5134	subash@gmail
Ejamaana.pdf	58482	66632	CSP8241	subash1996@g

File Status

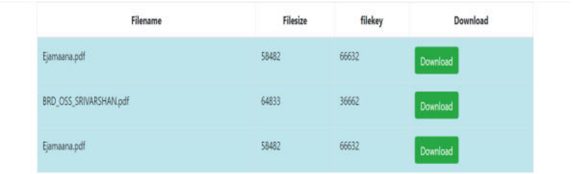
4. User

1. Users can either login if User has already registered or user can signup to create an account.

2. Now users can view files that are available in the database.

3. Now the user can search for it and request the key for it.

4. Once after getting a key from Admin, the user can successfully enter the first key and second key will be sent to user mail for the confidential purpose , it will be available only if the Auditor accepts the request from the user.



Filename	Filesize	filekey	Download
Ejamaana.pdf	58482	66632	Download
BRD_OSS_SRIVARSHAN.pdf	64833	36662	Download
Ejamaana.pdf	58482	66632	Download

File Download and key as Two Step authentication

CONCLUSION

We proposed a solution for end users to exploit the usage of cheap Cloud storage services while keeping their data safe. Our method can be applied on many different data formats which significantly improved the concept of selective encryption by introducing fragmentation and dispersal methods. The experimental and theoretical results have verified that our method can provide a high level of protection with resistance against propagation errors. We also provided a fast runtime on different PC platforms with practical designs and implementations based on GPGPU acceleration. In summary, we proposed a secure and efficient data protection method for end users to securely store the data on Clouds.

REFERENCE

[1] F. Hu, M. Qiu, J. Li, T. Grant, D. Taylor, S. McCaleb, L. Butler, and R. Hamner , “A review on cloud computing: Design challenges in architecture and security,” Journal of computing and information technology, vol. 19, no. 1, pp. 25–55, 2011.

[2] H. Li, K. Ota, and M. Dong, “Virtual network recognition and optimization in an SDN-enabled cloud environment,” IEEE Transactions on Cloud Computing, 2018.

[3] Y. Li, W. Dai, Z. Ming, and M. Qiu, “Privacy protection for preventing data over- collection in smart cities,” IEEE Transactions on Computers, vol. 65, no. 5, pp. 1339–1350, 2016.

[4] L. Kuang, L. Yang, J. Feng, and M. Dong, “Secure tensor decomposition using fully homomorphic encryption scheme,” IEEE Transactions on Cloud Computing, 2015.

[5] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "Big data analysis based secure cluster management for optimized control planes in software-defined networks," IEEE Transactions o n Network and Service Management, vol. 15, no. 1, pp. 27–38, 2018.

[6] K. Gai, K.-K. R. Choo, M. Qiu, and L. Zhu, "Privacy-preserving content-oriented wireless communication in Internet-of-Things," IEEE Internet of Things Journal, vol. 5, no. 4, pp . 3059–3067, 2018.

[7] S. Hambleton et al., "A glimpse of 21st century care," Australian Journal of General Practice, vol. 47, no. 10, pp. 670–673, 2018.

[8] K. Gai and M. Qiu, "Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers," IEEE Transactions on Industrial Informatics, 2017.

[9] O. Solon and O. Laughland, "Cambridge analytica closing after facebook data harvesting scandal," The Guardian, 2018.

[10] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.- J. Quisquater, "Overview on selective encryption of image and video: challenges and perspectives," EURASIP Journal on Information Security, vol. 2008, no. 1, p. 1, 2008.

[11] T. Xiang, J. Hu, and J. Sun, "Outsourcing chaotic selective image encryption to the cloud with steganography," Digital Signal Processing, vol. 43, pp. 28–37, 2015.

[12] H. Qiu, G. Memmi, X. Chen, and J. Xiong, "DC coefficient recovery for JPEG images in ubiquitous communication systems," Future Generation Computer Systems, 2019.

[13] G. O. Karame, C. Soriente, K. Lichota, and S. Capkun, "Securing cloud data under key exposure," IEEE Transactions on Cloud Computing, 2017.

[14] H. Qiu and G. Memmi, "Fast selective encryption methods for bitmap images," International Journal of Multimedia Data Engineering and Management (IJMDEM), vol. 6, no. 3, pp. 51–69, 2015.