Secure Data Outsourcing on Cloud Using Secret Sharing Scheme

Arup Kumar Chattopadhyay[1], Amitava Nag[2] and Koushik Majumder[3]
(Corresponding author: Arup Kumar Chattopadhyay)
Department of Computer Science and Engineering, Academy of Technology[1]
Adisaptagram, Aedconagar, Hooghly 712121, West Bengal, India
Department of Information Technology, Central Institute of Technology[2]
Kokrajhar 783370, BDAT, Assam, India
Maulana Abul Kalam Azad University of Technology, West Bengal, India[3]
(Email: ardent.arup@gmail.com)
(Received July 12, 2016; revised and accepted Nov. 15 & Dec. 25, 2016)

Abstract

Data Outsourcing in Cloud (DOC) has its exclusive benefits like low-cost, lower management overhead, elasticity of storage etc and these encourage organizations to use cloud computing to outsource massive amount of data to the cloud providers. The outsourced environment of the cloud and its inherent loss of control cause risk of exposing highly sensitive data to internal or external attacks. Traditionally, the data are kept encrypted to have secure authorized-only access. But, encrypting and decrypting large data files are computationally costly. Hence, secret sharing based DOC schemes have emerged due to their low complexity. Here, the proposed scheme uses simple Boolean based encryption and decryption of the data files (only image-files are considered in this paper) which is low in computational cost. The encrypted data files will be shared on the cloud. A threshold (t, n)-secret sharing scheme applied on the symmetric key of the encryption algorithm. The n share-keys will be generated from the secret key and will be distributed among participants. If t or more ($\leq n$) shared-keys are submitted, the original data files can be retrieved. Hence, it allows a threshold authorized-group of t or more data-users.

Keywords: Cloud Computing; DOC; Image Encryption; Secret Sharing

1 Introduction

Cloud computing was primarily developed for resource sharing with the motive of high availability, scalability, efficiency, cost-effectiveness of deploying utilities on network. Today cloud is a cost effective, flexible and on demand service delivery platform for providing business online. The key benefits of cloud computing are as follow:

1) Rapid Deployment: Deployment of hardware and software resources on cloud is on demand.
2) Availability: Resources on cloud is available anytime and anywhere.
3) Cost Reduction: It reduces the cost invested on hardware and software.
4) Scalability: Cloud can scale up or down its availability of resources like storage, computing depending on the varying needs of client.
5) Efficiency: Sharing the resources on cloud also provides an optimal utilization of resources.
6) Easier Collaboration: The resources shared on cloud can be accessed by many users at the same time from heterogeneous platforms. Thus it provides a collaborative approach for resource use.

Authors in [9] have described the key characteristics of cloud technology such as Multi-tenancy, Massive Scalability, Rapid Elasticity, Measured Service etc.

Data Outsourcing in Cloud (DOC) is a new paradigm where data are stored onto a trusted third-party service provider, such as cloud file server, cloud data server etc. The benefits of DOC as described in [5, 35] are on-demand and high quality service, universal data access by data-users regardless of their location and cost reduction in hardware and software resources.

Security remains the critical issue for the data outsourced on cloud. Data owner leverages on the service provider's hardware and software for storing and managing the outsourced data because it is a cost-effective and efficient solution, but at the same time the data owner loses control over the sensitive or confidential data which may be disclosed to unauthorized users [8]. As a result some customers are unwilling or unable to entrust their raw sensitive data to cloud providers. Authors in [16, 21]

have discussed the security issues for cloud. These issues include - cloud integrity, privacy, confidentiality and availability. The unique security requirements for cloud computing are identified in [43]. In such situation, different solutions for securing the confidentiality of the outsourced data has been developed. The authors in [11] discussed different types of attack on cloud which can be security threat for the outsourced data at cloud and authors in [4] have summarized the key strategies to be used to enhance the security of data stored at cloud environment and compare those techniques [29].

The traditional approaches used to secure the outsourced data on cloud are based on encryption. Both symmetric and asymmetric encryption schemes are used to conceal the original data and provide access structure to authorize the user to access the data. The use of encryption techniques to secure the data on cloud are discussed in [15, 20, 28, 34, 40, 46]. Vimercati et al. in [40] proposed a scheme where a two layer encryption is to be imposed on data to manage the access control on outsourced data. In 2007, Chase [10] has put forward Multi-Authority Authority Based Encryption (ABE), in this scheme a user is identified by a set of attributes and functions to determine the ability of the user to decrypt the cipher and it provides a fine grain access control. The scheme in [10] was improved by Li et al. [22] and defined with lesser ciphertexts and user's secret keys, along with ability to the encrypter to determine the number of attributes are desired for each ciphertext. The attribute based access control proposed in [20] is based ciphertext-policy attribute based encryption (CP-ABE) to enforce access control policies with efficient attribute and user revocation capability. Lu et al. in [28] proposed fine grained content level access control by hiding the paintext data content and issuing search token with decryption keys. Raykova et al. in [34] proposed a two-level access control scheme which handles both read and write access control for data users and data owners. Zhou et al. in [46] have proposed a tree-based key management scheme that allows the outsourced data to be accessed by multiple parties who hold different rights. Tree-based key management method of access hierarchies for data outsourcing is also discussed by W. Wang et al. in [41]. The authors in [12] have proposed a new public-key cryptosystems (that compress secret keys) that produce constant size ciphertext and enable efficient delegation of decryption rights for any set of ciphertexts. Giweli et al. [15] proposed a secure DOC method based on a combination of cryptography techniques, including the Chines Remainder Theorem, symmetric and asymmetric encryption. Fu et al. in [14] proposed a verifiable outsourced ciphertext decryption based on prime order bilinear group which made the scheme efficient for data consumer.

Achieving confidentiality of outsourced data using encryption is not computationally efficient as the encryption/decryption operations are time consuming. Most of these schemes use specialized encryption with complex mechanism, ranging from order-preserving encryption [2], which has limited security but is highly efficient, to oblivious RAM [37], which has provable access pattern and is highly secure but with poor performance. In recent years, a number of DOC schemes have been proposed with secret sharing. The authors in [1, 18, 39] proposed secure data outsourcing with Shamir's threshold secret sharing scheme [36], in which the secret (the data file) will be encoded into n shares or pieces and those n shares or pieces will be kept on n different data-storage-servers in the cloud; knowledge of any t or more shares will retrieve the whole secret (data file). But, Dautrich and Ravishankar [13] have shown that these schemes are vulnerable to the collusive attack in which any t colluding servers can recover all the files outsourced to the cloud. Muhammad et al. in [30] proposed secure data outsourcing based on Asmuth-Bloom secret sharing scheme (Asumuth-Bloom used Chinese Remainder Theorem in their proposed scheme [6]). Authors in [3, 31, 33] proposed secret sharing for securing multi-cloud i.e. a collection of several cloud infrastructures. Another fast and secure data outsourcing scheme is proposed by Liu at el. [27] based on Shamir's secret sharing scheme. It split the data files into public and private shares. Public shares are available in the cloud where as private shares are with data users. If valid data users submit their private shares, then only full data file can be retrieved from the cloud.

We assume honest-but-curious server threat model, commonly used for data outsourcing in cloud. The objective of the scheme described in this paper, is to secure the outsourced data with the combined effect of encryption and secret sharing. The data to be outsourced will be encrypted with a key and the key will be shared by a secret sharing algorithm to generate a threshold access structure to retrieve the key in full. Hence, the permissible group having threshold number of members will be able to retrieve all the secrets, encrypted using the key.

The rest of the paper is organized as follows: Section 2 defines the entities from cloud computing and secret sharing to be used in our scheme, Section 3 describes the algorithms to be used at proposed scheme, Section 4 describes the proposed model, a few experimental results are shown in Section 5, the security analysis is there in Section 6, and the scheme in concluded at Section 7.

2 Preliminaries

The entities from the cloud computing and secret sharing schemes to be used in the proposed model are described as follows.

2.1 Entities of Cloud Computing

Data Owner. Data owner is the actual possessor of the sensitive and confidential data files to be outsourced on the cloud. The data owner does not prefer to store the raw data with trusted third-party server, rather the encrypted version - cipher-steam will be

outsourced and store at cloud data-storage-server.

Data User. Data user is the end-user trying to access the secure outsourced data on cloud. The data user must have enough privilege such that he/she will be called an authorized user permitted to access the secret data on cloud.

Cloud Storage Server. These are the collection of data-storage-servers in the cloud that stores the data files outsourced on the cloud and provides location transparency to the data owner and data users.

2.2 Entities of (t, n)-threshold Secret Sharing

Secret. In secret-sharing schemes, the secret S is the data or data file which must the secured from the unauthorized user or unauthorized group. In the proposed scheme, the secret S is the encrypted version of the data-file to the stored in cloud.

Shares. The secret S will be encoded in n pieces called shares or shadows. Knowledge of t or more shares ($\leq n$) reveal the secret in full, any less than t shares will not reveal any secret.

Dealer. Dealer is the owner of the secret, who generates the shares and distributes them among n participants.

Participants. The participants are the users seeking the secret. If t or more participants submit their shares the secret can be revealed.

Combiner. The combiner is responsible for decoding of the secret. If t or more shares are submitted to the combiner then the combiner can decode the secret. Otherwise no information about the secret can be revealed.

3 Related Works

The secret sharing scheme used in our proposed model is based on Shamir's (t, n)-threshold secret sharing (1979) [36] and Thien-Lin image secret sharing scheme (2002) [38] (which extended Shamir's scheme for secret image sharing (SIS)). In the following subsections we discuss Shamir's scheme and the image encryption scheme using affine transformation and XOR operations as proposed by Nag et al. [32].

3.1 Shamir's Secret Sharing Scheme

Shamir in [36] has proposed a $(t, n)-$ threshold secret sharing scheme based on Lagrange interpolation. In a $(t, n)-$ threshold secret sharing scheme, a secret S is encoded into n parts called shadows or shares and distributed among n participants or players. If any t (or more) shares are obtained then the full secret S can be reconstructed and no less than t shares can reconstruct the secret or expose any information about the secret. As the decoding criteria depends on minimum number (t) of participants who can reconstruct the secret, t is called threshold. As proposed by Shamir, the (t, n)-threshold secret sharing scheme requires $(t-1)$ degree of polynomial:

$$q(x) = (a_0 + a_1 x + a_2 x^2, \cdots, a_{t-1} x^{t-1}) mod\ p, \quad (1)$$

where $a_0 = S$, the secret, p is a large prime, $a_0, a_1, \cdots, a_{t-1}$ are coefficients are in $GF(p)$.

Construction of Shares: The n shares s_i where $i = 1, 2, \cdots, n$ can be generated as follows:

$$s_1 = q(1), \cdots, s_i = q(i), \cdots, s_n = q(n).$$

Reconstruction of Secret: If t or more shares are submitted then the polynomial $q(x)$ can be regenerated by Lagrange interpolation theorem as follows:

$$q(x) = \sum_{j=1}^{t} s_j \prod_{m=1, m\neq j}^{t} \frac{x - x_m}{x_j - x_m} mod\ p.$$

The secret S can be determine as

$$S = q(0).$$

Several improvements have been proposed on the Shamir's scheme to detect and identify cheaters - disloyal participants who provide faked shares to deceive the honest participants (because they obtain an incorrect secret) or dishonest dealer supplies fake shares to the participants. Harn et al. [19] and Liu et al. [26] proposed verifiable secret sharing scheme based CRT and extended Asmuth-Bloom scheme. Those schemes are further improved by Liu et al. [25] by introducing single way hash function to ensure the secrecy maintained for both the shares and secret.

3.2 Image Encryption Using Affine Transform and XOR Operation

Nag et al. proposed an encryption scheme [32] in 2011 effective for images. The scheme considered eight 8-bit keys, say $K_0, K_1, K_2, K_3, K_4, K_5, K_6$ and K_7. The two-phase encryption process is as follows.

Phase 1: Redistribution of the pixels to the new locations using affine transformation with four keys breaks the strong correlation between the pixels. Let the old pixel position be (x, y), the translated location (x', y') can be calculated as

$$\begin{aligned} x' &= (K_0 + K_1 \times x) mod\ n \\ y' &= (K_2 + K_3 \times y) mod\ n. \end{aligned}$$

Phase 2: The image will be decomposed into $\frac{n}{2} \times \frac{n}{2}$ blocks recursively till each block will be of size (2×2). Encrypt the block pixels (p_1, p_2, p_3 and p_4) using keys - K_4, K_5, K_6 and K_7 as follows:

$$\begin{aligned} cp_1 &= p_1 \oplus K_4 \\ cp_2 &= p_2 \oplus K_5 \\ cp_3 &= p_3 \oplus K_6 \\ cp_4 &= p_4 \oplus K_7. \end{aligned}$$

Apply the procedure for all the blocks. The decryption can be done when all 8 keys are available.

Phase 1: The encrypted pixels in the blocks will be encrypted as

$$\begin{aligned} p_1 &= cp_1 \oplus K_4 \\ p_2 &= cp_2 \oplus K_5 \\ p_3 &= cp_3 \oplus K_6 \\ p_4 &= cp_4 \oplus K_7. \end{aligned}$$

Phase 2: The image pixels will be re-positioned as

$$\begin{aligned} x &= ((x' + (-K_0)) \times K_1^{-1}))mod\ n \\ y &= ((y' + (-K_2)) \times K_3^{-1}))mod\ n. \end{aligned}$$

The same scheme has been applied for the proposed model with some modification - (1) the key size is 16-bit consist of four 4-bit subkeys used for affine transformation, and (2) a key matrix of size the same size as the target image ($w \times h$) is used rather (2×2) matrix with four 8-bit keys; the key matrix directly gets XORed with the target image.

4 Proposed Model

Let the m secret images are $SI_1, SI_2, \cdots, SI_m$ of fixed size $w \times h$ and a random matrix R (Combiner Secret) of same size. Let number of participants be n. The objective is that if any t or more participants ($\leq n$) submit their keys then all the images can be retrieved. The phases are as follows.

4.1 Encryption of Secret Images and Distribution of Secret Keys

Step 1: The data owner submit m secret images to the dealer. The dealer encrypts the secret images SI_i, $\{i = 1\ to\ m\}$ with combiner secret R and a 16-bit key K (having four 4-bit subkeys - k_1, k_2, k_3, and k_4). The encoded images EI_i are generated as follows: For each image SI_i in $i = 1, 2, \cdots, m$ apply affine transformation as

$$\begin{aligned} x' &= (k_1 + k_2 \times x)mod\ w \\ y' &= (k_3 + k_4 \times y)mod\ h \end{aligned}$$

where (x, y) is the old pixel position and (x', y') is the new position. Then, the translated images, SI_i' will be XORed with R as

$$EI_i = SI_i' \oplus R, \quad \{for\ i = 1\ to\ m\}.$$

Step 2: The encoded images will be stored in cloud and the combiner secret R will be encrypted (with affine transformation) to C_R with a key k_1, k_2, k_3, k_4 and will be stored with the combiner. For each pixel position (x, y) of R, calculate the translated position (x', y') using affine translation.

$$\begin{aligned} x' &= (k_1 + k_2 \times x)mod\ w \\ y' &= (k_3 + k_4 \times y)mod\ h. \end{aligned}$$

Step 3: Generate n shares $sk_1, sk_2, \cdots, sk_n$ from the 16-bit key, K using *Shamir Secret Sharing Scheme*.

Step 4: Distribute key shares sk_i to P_i for $i = 1, 2, \cdots, n$.

4.2 Retrieval of Secret Images

Step 1: Let t or more participants ($\leq n$) submit their key shares sk_i to the Combiner.

Step 2: Combiner uses *Shamir's (t, n)-threshold Secret Sharing Scheme* to reconstruct the secret key, K. Thus, from K, four 4-bit subkeys- k_1, k_2, k_3, k_4 become available now.

Step 3: The encrypted combiner secret C_R will be decrypted with k_1, k_2, k_3, k_4 and the combiner key R will be retrieved as

$$\begin{aligned} x &= (x' + (-k_1)) \times k_2^{-1})\ mod\ w \\ y &= (y' + (-k_3)) \times k_4^{-1})\ mod\ h. \end{aligned}$$

Step 4: Combiner fetches all m encoded images, EI_i and decodes them as follows: First, EI_i will be XORed with R:

$$SI_i' = EI_i \oplus R, \quad \{for\ i = 1\ to\ m\}$$

Then, apply affine re-translation for each SI_i' for $i = 1, 2, \cdots, m$ as

$$\begin{aligned} x &= (x' + (-k_1)) \times k_2^{-1})\ mod\ w \\ y &= (y' + (-k_3)) \times k_4^{-1})\ mod\ h \end{aligned}$$

where (x, y) is the original location of the pixel.

Step 5: The decoded images will be made available to the t or more requesting participants.

A comparative study between different encryption schemes proposed for DOC is show in Table 1.

Table 1: Comparisons between proposed encryption scheme with other related scheme

Schemes	Decryption key size	Cipher-text size	Encryption type
Proposed Scheme	key-size for affine transformation is fixed; key-size for XOR is in $O(plaintext)$	$O(plaintext)$	symmetric-key
Key assignment schemes for a predefined hierarchy in [24]	depends on the hierarchy	$O(plaintext)$	symmetric or public-key
Symmetric-key encryption with Compact Key in [7]	fixed	$O(plaintext)$	symmetric-key
Attribute-Based Encryption in [17]	variable size	$O(plaintext)$	public-key
Key-Aggregate Cryptosystem based Encryption in [12]	fixed	$O(plaintext)$	public-key

5 Observations

Consider the secret image SI (as shown in Figure 1a) which has to be uploaded in the cloud. Consider a 16-bit key, $K = 20715$ (0110101110000101) as secret, $S = K$. Using Shamir's (t, n)-threshold secret sharing scheme where $n = 5, t = 3$, the shares are generated as follows:

$$s_1 = 20748 \quad (0001100001000101),$$
$$s_2 = 20805 \quad (0101000101000101),$$
$$s_3 = 20886 \quad (0011010011000101),$$
$$s_4 = 20991 \quad (0111111111000101),$$
$$s_5 = 21120 \quad (0000000010100101).$$

The subkeys used for encryption from key K are - k_1, k_2, k_3 and k_4 as follows:

$$\begin{aligned} k_1 &= 0110 = 6, \\ k_2 &= 1011 = 11, \\ k_3 &= 1000 = 8, \\ k_4 &= 0101 = 5. \end{aligned}$$

Consider combiner secret R (random matrix of the size of original image) as shown in Figure 1b. Use the combiner secret R to encrypt the original image SI. The result encrypted image shown in Figure 1c.

Applying Affine transformation to translate the pixel positions with keys k_1, k_2, k_3 and k_4 we get the encrypted image shown in Figure 1d. The Combiner Secret, R is also encrypted by keys, k_1, k_2, k_3 and k_4 to generate the encrypted version of Combiner Secret, C_R and will be stored with the Combiner.

Considering any 3 shares say, s_1, s_2, s_3 the key K and the subkeys are reconstructed as: $K = 20715$ $(k_1 = 0110 = 6;\ k_2 = 1011 = 11;\ k_3 = 1000 = 8;\ k_4 = 0101 = 5)$.

Using the keys Combiner perform affine transformation to re-translate the pixels to reconstruct the Combiner Secret R from C_R. The same keys are used to re-translate the encrypted image, as shown in Figure 2a.

Use Combiner Secret R to farther decrypt the image. The obtained image is shown in Figure 2b.

6 Security Analysis

The original image and the final encrypted image are as shown in Figure 3a and Figure 3b respectively.

6.1 Key Space Analysis

To resist brute force attack the key space should be large enough to make the attack infeasible. In proposed scheme, the key used for the XOR operation is the same size of the image i.e. $w \times h$. Hence, the key space will be $2^{w \times h}$. So, for a very small image of (64×64), they key space is $2^{64 \times 64}$, which is quite large. Affine cipher is created by 4 keys each of size 4 bits, key space for affine translation is 2^{16}. So, total key space will be $2^{(16 \times w \times h)}$, which is large enough if the image is not extremely small.

6.2 Statistical Analysis

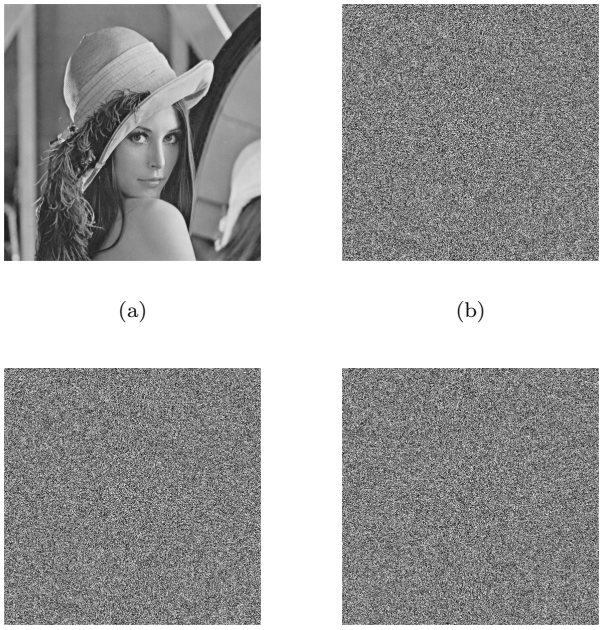
To resist statistical attacks, large amount of diffusion and confusion needs to be introduced in the cipher image. The following are the statistical analysis to ensure that it can prevent statistical attacks.

6.2.1 Histograms of Corresponding Images

Histogram of a given image reflects the distribution information of the pixel values. The histogram of an ideal encrypted image should have a uniform distribution and it will be completely different from the histogram of the plain-image. Histograms of the (512×512) grayscale image (of Lena.tif) and the cipher image are as shown in figures 4a and 4b. It is clearly visible that the histogram of the ciphered image in Figure 4b is fairly uniformly distributed, this is important in resisting statistical analysis attack.

6.2.2 Correlations of Two Adjacent Pixels

In a plain-image the adjacent pixels are highly correlated in either horizontal, vertical or diagonal direction. It is an important challenge for an encryption technique to reduce the correlation significantly in cipher image. To test the correlation of plain-image and cipher-image, the



(a) (b)

(c) (d)

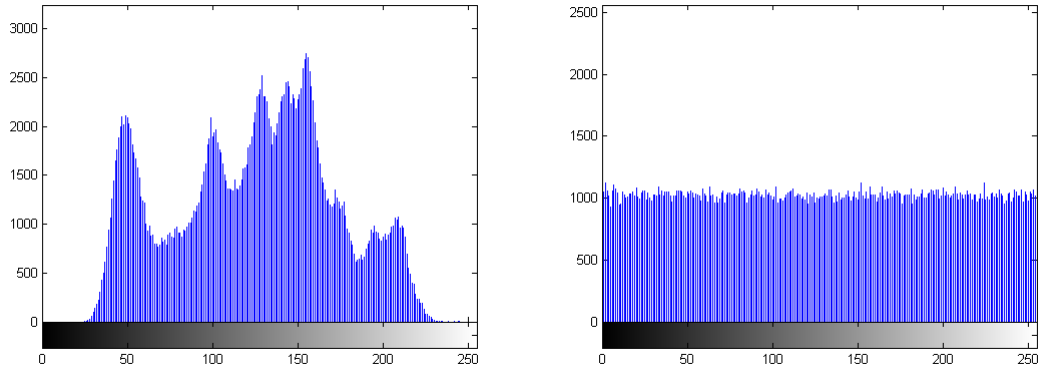
Figure 1: Construction of the encrypted image - (a) is the original image; (b) Combiner Secret R; (c) image after XORed with Combiner Secret R; (d) image after affine translation (this is the final image to be uploaded on cloud)

(a) (b)

Figure 2: Reconstruction of the secret image.(a) image after affine re-translation of the pixels; (b) image after XORed with Combiner Secret R

(a) (b)

Figure 3: (a) is the original image; (b) final encrypted image



(a) (b)

Figure 4: (a) is the histogram of the original image; (b) is the histogram of the final encrypted image

correlation coefficients of the adjacent pixels in vertical, horizontal and diagonal directions are evaluated by using following equations:

$$
\begin{aligned}
r_{xy} &= \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \\
E(x) &= \frac{1}{S}\sum_{i=1}^{S} x_i, \\
D(x) &= \frac{1}{S}\sum_{i=1}^{S}(x_i - E(x))^2, \\
cov(x,y) &= \frac{1}{S}\sum_{i=1}^{S}(x_i - E(x))(y_i - E(y)),
\end{aligned}
$$

where x and y are gray values of adjacent pixels and S is total number of duplets (x, y) obtained from image. $E(x)$ and $D(x)$ are the expectation and variance of x, respectively. As shown in Table 2, there is high correlation in the original image, but correlation in cipher image is negligible. Comparison between proposed scheme with few important encryption schemes (with respect to correlation-values) is shown in Table 2.

6.2.3 Information Entropy Analysis

The information entropy is the indicator of the randomness in the image, which can be calculated as

$$H(s) = \sum_{i=0}^{2^{N-2}} p(s_i) log_2 \frac{1}{p(S_i)},$$

where $p(s_i)$ is the probability of variable $s(i)$. For true random source producing 2^L, the entropy should be L. For, a gray-scale image with 8-bit pixels can have 2^8 different values (that is 0 to 255). Thus, entropy of a true random image must be 8. A close value of 8 of information entropy for a cipher image indicates, it is random enough.
Information Entropy Analysis for Lena.tif (512×521)

Entropy value of Original Image	=	7.4451
Entropy value of Cipher Image	=	7.9992

6.2.4 Sensitivity Analysis

Sensitivity analysis is another measure of randomness, have two indicators (1) NPCR (number of pixels change rate) and (2) UACI (unified average changing intensity). NPCR and UACI are computed by the following equations:

$$
\begin{aligned}
NPCR &= \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \\
UACI &= \frac{1}{W \times H}\sum_{i,j}\frac{|c_1(i,j) - c_2(i,j)|}{255} \times 100
\end{aligned}
$$

where c_1 and c_2 are two images of size $W \times H$. If $c_1(i,j) \neq c_2(i,j)$, then $D(i,j) = 1$, otherwise $D(i,j) = 0$.
Sensitivity Analysis for Lena.tif (512×521)

NPCR Score	=	0.996105194091797
UACI Score	=	0.286168850169462

NPCR and UACI values of proposed image encryption and few other important encryption schemes are as shown in Table 3.

6.3 Security Analysis of Data Outsourced at Cloud

The following are few security requirements (known as CIA) to be satisfied by DOC.

Data Confidentiality. The outsourced data on cloud should not be revealed to an unauthorized data user or data group. In the proposed (t,n)-scheme, a threshold group of t or more data-users only can access the outsourced data. But, as the scheme is applied on the symmetric keys, not on the data-file, the scheme cannot provides access transparency for

Table 2: Correlation coefficients of two adjacent pixels in three directions

Image (Scheme)	Horizontal	Vertical	Diagonal
Original image	0.97192828	0.98502945	0.95933083
Cipher image (using Proposed Scheme)	0.00201878	0.00136410	0.00186629
Cipher image (using Zhu's Scheme ([47])	0.00201613	0.00091642	0.00165094
Cipher image (using Zhang's Scheme ([45]))	0.00243875	0.00064593	0.00124402
Cipher image (using Wang's Scheme ([42]))	0.00190641	0.00381759	0.00194828

Table 3: Performance of different algorithms

Algorithm	NPCR	UACI
Proposed algorithm	0.996105194	0.286168850
Wang's algorithm in [42]	0.995864868	0.332533000
Zhang's algorithm in [44]	0.995998382	0.310221067
Zhu's algorithm in [47]	0.811958313	0.273860931
Lian's algorithm in [23]	0.033283200	0.007984160

data-files (data-user know the file which content the desired data).

Data Integrity. The outsourced data must be revealed in full to an authorized data-user or data-group whereas no part of the secret data will be revealed to the unauthorized-user or data-group. In the proposed scheme, a group of t or more data-users are authorized to access the data-files, whereas no part of data-file will be revealed to a group consists of less than t users.

Data Availability. Availability of data-files means that the data outsourced on the cloud must be available when required. In our proposed scheme, the same can be achieved by replicating the data-files in cloud.

A common threat to the DOC using secret sharing is described as Collusive attack (in [13]), where multiple cloud storage-servers can collude and can reveal the secret which none of them can do individually. A DOC scheme must be *Collusion-resistance*. In our proposed scheme the data-file is encrypted, where as the key is encoded in n shares and secretly distributed to the n data-users, so collusive attack is not applicable. A comparative study between DOC schemes [1, 18, 27, 39] using secret sharing is as shown in Table 4.

7 Conclusion

The confidentiality and security of the outsourced data on cloud is the concern of the day. Encryption based approaches are computationally inefficient and secret sharing based approaches are threatened by limited security of colluding servers. Thus, the proposed model is a combination of encryption and secret sharing. The data files (only images are considered in the proposed model) are encrypted by simple XOR and affine transformation of pixels' positions which are efficient in term of computation and the encryption key is shared by Shamir's threshold secret sharing scheme, which creates a threshold access structure of the data users. If the threshold or more number of participants submit their keys the data-files can be retrieved in full.

References

[1] D. Agrawal, A. E. Abbadi, F. Emekci, A. Metwally, and S. Wang, "Secure data management service on cloud computing infrastructures," in *Proceeding of the Service and Application Design Challenges in Cloud*, pp. 57–80, 2011.

[2] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *Proceedings of the 2004 ACM SIGMOD international conference on Management of data*, pp. 563–574, Paris, France, June 2004.

[3] M. K. Alam and S. Banu, "An approach secret sharing algorithm in cloud computing security over single to multi clouds," *International Journal of Scientific and Research Publications*, vol. 3, no. 4, pp. 1–5, 2013.

[4] S. L. Anil and R. Thanka, "A survey on security of data outsourcing in cloud," *International Journal of Scientific and Research Publications*, vol. 3, no. 2, pp. 1–3, 2013.

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: a berkeley view of cloud computing," Tech. Rep. UCB/EECS-2009-28, Feb. 2009.

[6] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 208–210, 1983.

[7] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: Ensuring privacy of

Table 4: Comparison between different SSS-based DOC schemes

Schemes	Data Confidentiality	Data Correctness	Collusion Resistance	Number of public shares	Round of transmission	Types
Proposed Scheme	Yes	Yes	NA	1	1	(t,n)-SSS based
[27]	Yes	Yes	Yes	$n-1$	l	(t,n)-SSS based
[39]	Yes	Yes	No	$l \times t$	l	(t,n)-SSS based
[1]	Yes	Yes	No	$l \times t$	l	(t,n)-SSS based
[18]	Yes	Yes	No	$l \times t$	l	(t,n)-SSS based

electronic medical records," in *Proceedings of the 2009 ACM workshop on Cloud computing security (CCSW'09)*, pp. 103–114, Chicago, IL, USA, Nov. 2009.

[8] Z. Cao, C. Mao, L. Liu, "Analysis of one secure anti-collusion data sharing scheme for dynamic groups in the cloud," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 68–72, 2016.

[9] S. Carlin and K. Curran, "Cloud computing technologies," *International Journal of Cloud Computing and Services Science*, vol. 1, no. 2, 2012.

[10] M. Chase, "Multi-authority attribute based encryption," in *Proceeding of the 4th conference on Theory of cryptography (TCC'07)*, pp. 515–534, Amsterdam, Netherlands, Feb. 2007.

[11] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: Outsourcing computation without outsourcing control," in *Proceedings of the 2009 ACM workshop on Cloud computing security (CCSW'09)*, pp. 85–90, Chicago, IL, USA, Nov. 2009.

[12] C. K. Chu, S. S. M. Chow, W. G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," *IEEE Transactions on Parallel and Distributed System*, vol. 25, no. 2, pp. 468–477, 2014.

[13] J. L. Dautrich and C. V. Ravishankar, "Security limitations of using secret sharing for data outsourcing," in *Proceeding of the IFIP Annual Conference on Data and Application Security and Privacy*, pp. 145–160, Paris, France, 2012.

[14] X. Fu, X. Nie, and F. Li, "Outsource the ciphertext decryption of inner product predicate encryption scheme based on prime order bilinear map," *International Journal of Network Security*, vol. 19, no. 2, pp. 313–322, 2017.

[15] N. Giweli, S. Shahrestani, and H. Cheung, "Enhancing data privacy and access anonymity in cloud computing," *Communications of the IBIMA*, vol. 2013, no. 462966, pp. 1–10, 2013.

[16] A. Goel and S. Goel, "Security issues in cloud computing," *International Journal of Application or Innovation in Engineering & Management*, vol. 4, no. 1, pp. 121–124, 2012.

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Multi-identity single-key decryption without random oracles," in *Proceedings of the 3rd SKLOIS Conference (Inscrypt 2007)*, pp. 89–98, Alexandria, Virginia, USA, Oct. 2006.

[18] M. A. Hadavi and R. Jalili, "Secure data outsourcing based on threshold secret sharing; towards a more practical solution," in *Proceedings of the 36th International Conference on Very Large Data Bases*, pp. 54–59, Singapore, Sept. 2010.

[19] L. Harn, M. Fuyou, and C. C. Chang, "Verifiable secret sharing based on the chinese remainder theorem," *Security and Communication Networks*, vol. 7, no. 6, pp. 950–959, 2014.

[20] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214–1221, 2011.

[21] R. Kumar, "Cloud computing and security issue," *International Journal Of Engineering And Computer Science*, vol. 5, no. 11, pp. 18823–18826, 2016.

[22] K. Li and H. Ma, "Outsourcing decryption of multi-authority abe ciphertexts," *International Journal of Network Security*, vol. 16, no. 4, pp. 286–294, 2014.

[23] S. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," *Chaos, Solitons & Fractals*, vol. 26, no. 1, p. 117–129, 2005.

[24] S. Lian, J. Sun, and Z. Wang, "Dynamic and efficient key management for access hierarchies," *ACM Transactions on Information and System Security*, vol. 12, no. 3, pp. 18:1–18:43, 2009.

[25] Y. Liu and C. C. Chang, "An integratable verifiable secret sharing mechanism," *International Journal of Network Security*, vol. 18, no. 4, pp. 617–624, 2016.

[26] Y. Liu, L. Harn, and C. C. Chang, "A novel verifiable secret sharing mechanism using theory of numbers and a method for sharing secrets," *International Journal of Communication Systems*, vol. 28, no. 7, pp. 1282–1292, 2015.

[27] Y. Liu, H. L. Wu, and C. C. Chang, "A fast and secure scheme for data outsourcing in the cloud," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 8, pp. 2708–2721, 2014.

[28] Y. Lu and G. Tsudik, "Enhancing data privacy in the cloud," in *Proceedings of the IFIP International Conference on Trust Management*, Singapore, 2011.

[29] A. Mosa, H. M. El-Bakry, S. M. Abd El-Razek, S. Q. Hasan, "A proposed E-government framework based

on cloud service architecture," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 93–104, 2016.

[30] Y. I. Muhammad, M. Kaiiali, A. Habbal, A. S. Wazan, and A. S. Ilyasu, "A secure data outsourcing scheme based on asmuthbloom secret sharing," *Enterprise Information Systems*, vol. 16, no. 4, pp. 1–23, 2016.

[31] M. Muhil, U. H. Krishna, R. K. Kumar, and E. A. M. Anita, "Securing multi-cloud using secret sharing algorithm," *Procedia Computer Science*, vol. 50, pp. 421–426, 2015.

[32] A. Nag, J. P. Singh, S. Khan, S. Biswas, D. Sarkar, and P. P. Sarkar, "Image encryption using affine transform and xor operation," in *Proceedings of the International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN'11)*, Singapore, July 2011.

[33] P. Pareek, "Cloud computing security from single to multi-clouds using secret sharing algorithm," *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 2, no. 12, pp. 3261–3264, 2013.

[34] M. Raykova, H. Zhao, and S. M. Bellovin, "Privacy enhanced access control for outsourced data sharing," in *Proceeding of the Financial Cryptography and Data Security*, pp. 223–238, Kralendijk, Bonaire, Feb. 2012.

[35] M. N. O. Sadiku, S. M. Musa, and O. D. Momoh, "Cloud computing: opportunities and challenges," *IEEE Potentials*, vol. 33, no. 1, pp. 34–36, 2014.

[36] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[37] E. Stefanov, E. Shi, and D. Song, "Towards practical oblivious ram," *Cryptography and Security*, pp. 1–40, 2012.

[38] C. C. Thien and J. C. Lin, "Secret image sharing," *Computers and Graphics*, vol. 26, no. 5, p. 765–770, 2002.

[39] X. Tian, C. F. Sha, X. L. Wang, and A. Y. Zhou, "Privacy preserving query processing on secret share based data storage," in *Proceeding of the 16th International Conference on Database Systems for Advanced Applications, (DASFAA'11)*, pp. 108–122, Hong Kong, China, Apr. 2011.

[40] S. D. C. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in *Proceedings of the 33rd International Conference on Very Large Data Bases (VLDB'07)*, pp. 123–134, Vienna, Austria, Sept. 2007.

[41] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in *Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW'09)*, pp. 55–66, Chicago, IL, USA, Nov. 2009.

[42] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Optics and Lasers in Engineering*, vol. 66, pp. 10–18, 2015.

[43] M. Zareapoor, P. Shamsolmoali, and M. A. Alam, "Establishing safe cloud: Ensuring data security and performance evaluation," *International Journal of Electronics and Information Engineering*, vol. 1, no. 2, pp. 88–99, 2014.

[44] Y. Q. Zhang and X. Y. Wang, "A symmetric image encryption algorithm based on mixed linearnonlinear coupled map lattice," *Information Science*, vol. 273, no. 20, pp. 329–351, 2014.

[45] Y. Q. Zhang and X. Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Applied Soft Computing*, vol. 26, pp. 10–20, 2015.

[46] M. Zhou, Y. Mu, W. Susilo, J. Yan, and L. Donga, "Privacy enhanced data outsourcing in the cloud," *Journal of Network and Computer Applications*, vol. 35, no. 4, pp. 1367–1373, 2012.

[47] Z. L. Zhua, W. Zhangc, K. W. Wongb, and H. Yua, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Science*, vol. 181, no. 6, p. 1171–1186, 2011.

Biography

Arup Kumar Chattopadhyay has received his BE degree from Visvesvaraya Technological University, Belgaum in 2002 and MTech. degree from University of Calcutta, Kolkata in 2011. He is currently associated with Academy of Technology, India as Assistant Professor. His current research interest is in Information Security.

Dr. Amitava Nag is having 12 years of academic experience and at present is serving as Associate Professor at the Dept. of IT, Central Institute of Technology (CIT), Kokrajhar, India. Prior to joining CIT, he was associated with Academy of Technology, Hooghly as Associate Professor.He received his PhD in Engineering from the University of Kalyani, India. He holds M.Tech in Information Technology from the University of Calcutta, India. His research focuses on Information Security, Cloud Computing and Internet of Things (IoT). He has contributed to numerous research articles in various journals and conferences of repute and is also one of the authors of 5 books. He is a member of the Institution of Engineers.

Koushik Majumder has received his Ph.D from Jadavpur University, Kolkata. He obtained his B. Tech and M. Tech degrees from the University of Calcutta, Kolkata. He is currently associated with Maulana Abul Kalam Azad University of Technology (MAKAUT) as Assistant Professor. His current research interest includes Mobile Adhoc Network, Information Security, Cloud Computing etc.