A Modified Homomorphic Encryption Method for Multiple Keywords Retrieval

Xiaowei Wang[1], Shoulin Yin[1], Hang Li[1], Lin Teng[1], and Shahid Karim[2]
(Corresponding author: Shoulin Yin)
Software College, Shenyang Normal University[1]
Shenyang 110034, China
Department of Computer Science, ILMA University[2]
Karachi, Pakistan
(Email: 352720214@qq.com)
(Received Apr. 29, 2019; Revised and Accepted Nov. 5, 2019; First Online Apr. 19, 2020)

Abstract

Currently, many data owners choose to outsource the data storage to cloud service providers. Data owners store the local private data with plaintext form in the cloud server. It is difficult to guarantee the data privacy and security. So data owners usually encrypt the local private data and upload it into cloud server. The traditional multi-keyword ciphertext retrieval methods cannot take both accuracy and security into consideration. Therefore, we propose a modified homomorphic encryption method for multiple keywords retrieval in this paper. It can effectively solve the privacy leakage of search keywords problem. The retrieval performance is greatly improved in multi-keyword retrieval process. Experimental results show that this new scheme is more efficient and accurate than other ciphertext retrieval schemes.

Keywords: Homomorphic Encryption; Multi-keyword Ciphertext Retrieval; Private Data

1 Introduction

Cloud storage [16] is a new network storage technology which is the extension and development of cloud computing [3]. It uses the grid technology, distributed file system, cluster application, virtualization functions and software to control network in large-scale heterogeneous storage devices and provide on-demand services to remote users of mass data storage access and processing functions. Cloud storage greatly saves the cost of storage hardware and software, reduces the investment of maintenance personnel, and has outstanding advantages such as low cost and high utilization rate. At the same time, professional cloud storage service providers have unparalleled technology and management level [8, 11], which can provide users with better data security services such as redundant backup and disaster recovery. In order to prevent the disclosure of privacy, users usually encrypt the data and then upload them into the cloud storage platform, and keep the decryption key by themselves such as government documents, national medical and health data, business secrets related documents, personal privacy data, etc [7, 12]. However, the encrypted data will lose some characteristics of the original plaintext such as order and similarity. As a result, the traditional plaintext based retrieval schemes cannot work well in the encryption cloud storage system. For this reason, researchers propose a secure ciphertext based on retrieval problem. The method is divided into two classes:

1) The indexing file-based retrieval method [13, 18];

2) The matching-based retrieval method [14, 17]. However, the two methods either need to maintain complex index structure or have low retrieval efficiency, which is difficult to meet the retrieval requirements of massive ciphertext data in the cloud storage environment. The encrypted data also brings new problems. For example, how can data user retrieve the data of interest quickly when facing massive ciphertext data. A common solution is to use keywords for retrieval.

Single-keyword retrieval cannot meet the needs of users for accurate retrieval, so the research of multi-keyword retrieval emerges at the right moment. Lu [9] proposed a secure sorting keyword retrieval algorithm, scoring documents containing keywords, and using one-to-many order-preserving mapping algorithm to encrypt data. The scheme improved the retrieval efficiency, but reduced the security of data and the precision of retrieval. Li [4] proposed a multi-keyword based on Boolean query scheme, which generated search results based on whether or not the keyword was included. However, this scheme could not distinguish the degree of relevance of multiple documents containing the same keyword. Hu [2] proposed a multi-keyword searchable public key encryption scheme,

but it was later proved that it could not resist keyword guessing attacks. Teng [6] proposed a secure ordering multi-keywords retrieval algorithm, and adopted the coordinate calculation keyword matching scheme and the correlation between document, using the inner product similarity evaluation of correlation between keywords, but the solution method of Boolean made documents that contained the same number of keywords score the same, with no guarantee of accuracy. Therefore, we propose an modified homomorphic encryption method for multiple keywords retrieval in this paper. It can effectively solve the privacy leakage of search keywords problem. The retrieval performance is greatly improved in multi-keyword retrieval.

2 Preliminaries

2.1 Homomorphic Encryption

Homomorphic encryption [5, 19] is an encryption method that can directly process ciphertext data. Under the premise of effectively protecting the privacy of user sensitive data, the homomorphic operations such as addition and multiplication can be directly implemented on the ciphertext, and maintain the plaintext order of the ciphertext when operating. However, homomorphic encryption scheme requires a great deal of computational overhead. How to design a homomorphic ciphertext retrieval scheme with less computational overhead and convenient for indexing is a difficult point in current research.

Using homomorphic encryption technology, it can guarantee the ciphertext algebraic operation results and the same in plaintext encrypted algebraic operation. That is, for any valid operation f and plaintext m, there is $f(Enc(m)) = Enc(f(m))$. This special property allows third parties to perform algebraic operations on ciphertext. No decryption is required. Its significance lies in fundamentally solving the confidentiality problem of data and its operation is entrusted to a third party. At present, there are three main frameworks for constructing full homomorphic encryption.

1) GCD problem. First, a partial homomorphic encryption scheme is constructed. And then the decryption circuit is compressed to perform homomorphic decryption of the ciphertext. So it can achieve the aim of controlling ciphertext noise growth. Finally, a fully homomorphic encryption scheme is obtained under the assumption of cyclic security.

2) R-LWE problem. First, a partial homomorphic encryption scheme is constructed [14]. After ciphertext calculation, key exchange is used to control the expansion of ciphertext vector dimension, and mode exchange is used to control the increase of noise. Without using homomorphic decryption technology, a layered all-homomorphic encryption scheme can be obtained.

3) LWE problem. The $N \times N$ matrix represents the ciphertext, and the key is a n-dimensional vector. The addition and multiplication of ciphertext matrix are still matrices, which will not lead to the change of dimension of ciphertext calculation result. If the ciphertext matrix is "strongly B-boundary", that is, the element in ciphertext C is at most 1, and the element in error e is at most B, then a hierarchical all-homomorphic encryption scheme that can execute polynomial depth can be obtained.

2.2 Retrieval Scheme based on Homomorphic Encryption

The retrieval scheme based on homomorphic encryption proposed in this paper consists of the following five modules:

1) $Init()$. The data owner at the client side produces the public key P_k, private key S_k of the homomorphic encryption algorithm according to the parameter λ. Initializing the key E_k of document encryption algorithm.

2) $Encrypt()$. The data owner generates document vector D according to document set (DS). The document vector D is encrypted using P_k to get D_{P_k}. The document set is encrypted with E_k to get DS_{E_k}. Upload encrypted data by calling the public API interface of the application interface layer.

3) $Query()$. Date user applies P_k, S_k and E_k for date owner. When data user performs the retrieval, the original retrieval vector is expanded to the standard retrieval vector Q to get Q_{P_k} by using P_k, and the application interface layer public API is called to submit the retrieval request.

4) $Score()$. After receiving the retrieval request, Cloud Server calculates the correlation score between the retrieval vector Q and document D in the ciphertext form, and returns the retrieval vector and the correlation score of each document to the client.

5) $TopK()$. Data user decrypts the returned score with S_k, runs $TopK$ algorithm to obtain K document numbers with the highest degree of relevance, and calls the public API of the application interface layer to request document data. The server receives the request to read the encrypted document from the storage layer and returns it to the client.

2.3 Correlation Score

The similarity between the query vector and the document vector reflects the matching degree of the keyword and the document of the user query, which is the basis of the retrieval and sorting. Query vector Q and document vector D have the same dimension I, this dimension corresponds to the total number of distinct feature items in

Table 1: Symbols in this paper

λ	Security parameter
ρ	The length of the noise. In order to resist violent attack, the noise length should be taken as $\rho = w \log \lambda$.
η	The binary length of the private key. Private key length satisfies $\eta \geq \rho\Theta(\lambda \log 2\lambda)$.
τ	The number of public key. $\tau \geq \gamma + w(\log \lambda)$.
γ	The binary length of the public key. Public key length satisfies $\gamma = w(\eta 2 \log \lambda)$.

all documents. The correlation scores of query vector Q and document vector D are expressed by the vector inner product as follows:

$$D_j = (w_{1j}, w_{2j}, \cdots, w_{lj}). \quad (1)$$

$$Q_q = (w_{1q}, w_{2q}, \cdots, w_{lq}). \quad (2)$$

$$Score = sim(Q_q, D_j) = \sum_{1}^{l} w_{iq} \cdot w_{ij}. \quad (3)$$

The the correlation score between query vector Q and document vector D is higher, the document D conforms to users' query requirements sharply. If the correlation score is lower, the document D meets the user's query requirements rarely.

3 Modified Homomorphic Encryption

The basic management of cloud storage provides ciphertext retrieval function. The relevant document number can be retrieved through the query conditions given by users. The ciphertext retrieval scheme designed in this paper is based on homomorphic encryption technology. Therefore, we give a modified homomorphic encryption scheme in this paper to provide more safe retrieval.

Firstly, the symbols used in this paper are explained as Table 1.

It includes four polynomial time operations: $Setup()$, $Encrypt()$, $Circuit()$, $Decrypt()$. The proposed scheme is valid.

1) $Setup(1^n, 1^l)$. Input security parameter $n = 2^k (k \in Z)$, maximum user number l and positive integer $p \leq q = 1 mod(2n)$, q is prime number. Randomly select $s \in R_q = Z_q[x]/ < f(x) >, f(x) = x^n + 1$ as private key. Public key is $a, b = a \cdot s + p \cdot e$. In here, $a \leftarrow R_q$ is uniformly selected. Error term e is independently selected from error distribution $\chi \subset R_q$.

2) $Encrypt(id, pk, m_i)$. Given the data identification id and the user's public key (a, b). In order to encrypt a $n - bit$ plaintext message $m_i \in 0, 1^n \subset R_p$, uniform randomly select $t_i \in R_q$. Output ciphertext $(c_i^1, c_i^2) = (a \cdot t_i + pe_i^1, b \cdot t_i + pe_i^2 + m_i)$, where $e_i^j (j = 1, 2)$ is independently selected from distribution χ.

3) $Circuit(id, \alpha_i, (c_i^1, c_i^2)_{i=1}^l)$. Input identification id, ciphertext $(c_1^1, c_1^2), \cdots, c_l^1, c_l^2$ with weight $\alpha_1, \cdots, \alpha_l$. Output ciphertext $(c^1, c^2) = (\sum_{i=1}^l \alpha_i c_i^1, \sum_{i=1}^l \alpha_i c_i^2) = (\sum_{i=1}^l \alpha_i (a \times t_i + pe_i^1, \sum_{i=1}^l \alpha_i (b \times t_i + pe_i^2 + m_i)$.

4) $Decrypt(id, sk, (c_1, c_2))$. After receiving the data id, the user's private key s_k and ciphertext (c_1, c_2), the plaintext $m = \sum_{i=1}^l \alpha_i m_i$ can be obtained by calculating $(c_2 - c_1 \cdot s) \bmod p$.

Theorem 1. *To decrypt the ciphertext, suppose the ciphertext is* $c^1, c^2 = \sum_{i=1}^l \alpha_i (a \times t_i + pe_i^1, \sum_{i=1}^l \alpha_i (b \times t_i + pe_i^2 + m_i)$, *then*

$$\begin{aligned}(c^2 - c^1 \cdot s) \bmod p &= \sum_{i=1}^{l} \alpha_i (b \times t_i + pe_i^2 + m_i) \\ &\quad - s \cdot \sum_{i=1}^{l} \alpha_i (a \times t_i + pe_i^1 \bmod p) \\ &= \sum_{i=1}^{l} \alpha_i [(a \cdot s + pe) \cdot t_i + pe_i^2 + m_i] \\ &\quad - \sum_{i=1}^{l} \alpha_i \cdot s(a \cdot t_i + pe_i^1) \bmod p \\ &= \sum_{i=1}^{l} \alpha_i m_i. \end{aligned} \quad (4)$$

So the proposed scheme is proofed. The encryption scheme is linearly homomorphic.

Proof. Known message $m_i \subset 0, 1^n \subset R_p$, and weight $\alpha_i (i = 1, \cdots, l$, according to $Encrypt$ algorithm, a linear combination $\sum_{i=1}^l \alpha_i m_i$ of the message m_i has the corresponding ciphertext $(a \times t + pe^1, b \times t + pe^2 + \sum_{i=1}^l \alpha_i m_i$. On the other hand, the corresponding ciphertext of the message m_i is $(c_i^1, c_i^2) = (a \cdot t_i + pe_i^1, b \cdot t_i + pe_i^2 + m_i)(i = 1, \cdots, l)$, then ciphertext (c_i^1, c_i^2) has the corresponding linear combination $(\sum_{i=1}^l \alpha_i c_i^1, \sum_{i=1}^l \alpha_i c_i^2)$. If the $Decrypt$ algorithm decrypts the ciphertext $(\sum_{i=1}^l \alpha_i c_i^1, \sum_{i=1}^l \alpha_i c_i^2)$, the corresponding plaintext $\sum_{i=1}^l \alpha_i m_i$ can be obtained. Obviously, the corresponding plaintext of the ciphertext $(a \cdot t + pe^1, b \cdot t + pe^2 + \sum_{i=1}^l \alpha_i m_i)$ also is $\sum_{i=1}^l \alpha_i m_i$. Therefore, the encryption scheme in this paper is linear homomorphic. □

Table 2: Performance comparison with dofferent schemes

Scheme	Mould exchange	Approximate eigenvectors	Start
DGHV	None	None	$O(\lambda^{14})$
BGV	$\tilde{O}(\lambda \cdot L^3)$	None	$\tilde{O}(\lambda^2)$
Bra12	None	None	$\tilde{O}(\lambda^6)$
GSW13	None	$\tilde{O}((nL)^w)$	$\tilde{O}(n(nL)^w)$
Proposed	None	$\tilde{O}(n^w)$	$\tilde{O}(n^w)$

4 Performance Analysis of Proposed Scheme

4.1 Security Analysis

Suppose that let the advantage of a PPT adversary A to correctly distinguish its corresponding plaintext through ciphertext be ε in the chosen plaintext attack. The attack model of A is as follows:

1) $Setup(1^n)$. The challenger runs $Setup(1^n)$ to get the key $s, (a, b = a \cdot s + pe)$ and sends the public key (a, b) to the adversary A.

2) $Queries$. A random selects $m_1, \cdots, m_{q_s}$ and sends them to challenger. The challenger computes $(c_i^1, c_i^2) = Encrypt(id, (a, b), m_i)(i = 1, \cdots, q_s)$ and send it to A.

3) $Challenge$. Once the $Queries$ is completed, A outputs two different plaintext m_0 and m_1 and sends them to the challenger, the only condition being that m_0 and m_1 are not queried. It randomly selects $b \in (0, 1)$ and will challenge the ciphertext $(c^1, c^2) = (a \cdot t + pe^1, b \cdot + pe^2 + m_b)$.

4) $Output$. A outputs the guess value b' of b.

If $b' = b$, the adversary A won this game, its probability is $Pr(b = b')$, the advantages of A is $Adv = |Pr(b = b') - \frac{1}{2}|$.

4.2 Keyword Retrieval Security

The retrieval request submitted by the user to the server is the ciphertext after the conversion of P, g and x. On the premise that P, g and x cannot be obtained, the keyword plaintext M cannot be obtained, which ensures the security of the user's keyword retrieval. At the same time, the server only operates on the ciphertext in the process of performing the retrieval, and cannot learn the plaintext of user data and keywords in the whole process, thus realizing the ciphertext retrieval function.

4.3 Security of Confidential Parameters

When generating system secret parameters, it must be considered that the key P must have enough key space to prevent the key P, g and x from being exhausted. However, the larger P is, the greater the overhead is. How to achieve a good balance between efficiency and security is one of the problems that this scheme needs to focus on.

4.4 Efficiency Analysis

The retrieval efficiency of proposed scheme is closely related to the keyword length. For files with fixed length, when the plaintext M is grouped, the grouping length is larger, the grouping division will be smaller, and the corresponding retrieval cycle times will be less. On the contrary, the more groups are divided, the more cycles needed in retrieval. Meanwhile, when grouping, it is possible to divide the keyword into different groups, which leads to the failure to correctly retrieve the keyword. Therefore, the retrieval accuracy is not 100%, but decreases with the increase of the number of groups. How to design a reasonable grouping length is also one of the difficulties in this scheme. In addition, because proposed scheme supports multi-keyword joint query, it can significantly improve the retrieval efficiency compared with other schemes.

4.5 Performance Analysis

The client initializes the key and establishes the vector space model only on time, so the performance of the retrieval scheme is mainly determined by the encryption query vector, score calculation and decryption calculation TopK module. Currently, there are four classical full homomorphic encryption schemes, namely, all-homomorphic encryption scheme (DGHV) on integer, modular exchange scheme (BGV) scheme, modular invariant scheme (Bra12) scheme and approximate eigenvector scheme (GSW13) scheme. Compared result of performance with our proposed shceme is given in Table 2.

5 Comparison Results

Through the establishment of indexes with different number of keywords, the retrieval efficiency of the scheme is tested and compared with three state-of-the-art methods WMF [10], FPH [1] and OCVR [15]. Taking 100 pure Chinese text documents as test samples, the average of each document is 2MB. In the test process, the keyword length is determined to be 2 Chinese characters, corresponding

Table 3: Time comparison with three schemes

Keyword number	WMF	FPH	OCVR	Proposed method
1	11.8ms	9.6ms	8.5ms	5.4ms.
2	15.7ms	12.5ms	10.7ms	7.6ms
3	18.3ms	15.8ms	13.6ms	9.4ms
4	21.3ms	18.5ms	15.3ms	11.4ms
4	24.6ms	21.7ms	19.7ms	15.9ms

Table 4: Retrieval accuracy rate comparison with three schemes

Keyword number	WMF	FPH	OCVR	Proposed method
1	89.6%	92.3%	95.7%	98.6%.
2	84.5%	91.1%	94.8%	97.5%
3	82.1%	88.5%	89.9%	94.3%
4	80.5%	86.7%	89.2%	93.2%
4	79.4%	82.4%	87.7%	90.1%

to 32-bit binary number. The number gradually increases from 1 to 5. 50 retrieval tests are performed for each index keyword number, and the average time is taken as the final result. The result is given in Table 3.

It can be seen that the keyword retrieval efficiency of the three schemes has big difference, and proposed scheme is slightly faster. But as the number of indexes increases, the time of proposed scheme grows more slowly.

As mentioned above, keywords may be divided into different groups in ciphertext grouping, resulting in the retrieval accuracy lower than 100%. The above 100 text documents are still taken as test samples to test the retrieval accuracy of proposed method. 10 different keyword combinations are randomly selected for each quantity, 50 tests are conducted and the average accuracy is recorded. The test results are shown in Table 4.

It can be seen that with the increase of the keywords number, the accuracy of proposed scheme decreases to a certain extent, the comprehensive retrieval accuracy is above 90%.

6 Conclusions

Compared with the traditional data storage, cloud storage has the characteristics of low cost, scalability, rapid scaling and high utilization rate, which makes cloud storage get more and more attention and support. However, if the security problems in cloud storage cannot be properly solved, especially the efficient ciphertext-based retrieval problem, it will seriously restrict the sustainable development of cloud storage applications. Aiming at this urgent problem, this paper proposes a new ciphertext retrieval mechanism based on full homomorphic encryption. By double ciphertext encryption mechanism, the ciphertext retrieval can be approximately accurate without recovering the encrypted plaintext information, and the ordering of the results can be realized. This scheme not only protects the user's data security, but also improves the retrieval performance of the full homomorphic encryption algorithms in multi-keyword retrieval, which has a certain application prospect.

Acknowledgments

This work is supported by the Natural Science Fund Guiding Program in Liaoning Province (Grant No.20180520024).

References

[1] S. Bai, Y. Geng, J. Shi, *et al.*, "Privacy-preserving oriented floating-point number fully homomorphic encryption scheme," *Security and Communication Networks*, vol. 1, pp. 1-14, 2018.

[2] C. Hu, B. Yang, P. Liu, "Multi-keyword ranked searchable public-key encryption," *International Journal of Grid & Utility Computing*, vol. 6, no. 3/4, pp. 221-231, 2015.

[3] C. Lan, H. Li, S. Yin, *et al.* "A new security cloud storage data encryption scheme based on identity proxy re-encryption," *International Journal of Network Security*, vol. 19, no. 5, pp. 804-810. 2017.

[4] R. Li, Z. Dong, Y. Zhang, *et al.* "Attribute-based encryption with multi-keyword search," in *IEEE Second International Conference on Data Science in Cyberspace*, 2017. DOI: 10.1109/DSC.2017.97.

[5] H. Li, S. L. Yin, C. Zhao and L. Teng, "A proxy re-encryption scheme based on elliptic curve group," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 218-227, Jan. 2017.

[6] T. Lin, L. Hang, L. Jie, Y. Shoulin, "An efficient and secure Cipher-Text retrieval scheme based on

mixed homomorphic encryption and multi-attribute sorting method under cloud environment," *International Journal of Network Security*, vol. 20, no. 5, pp. 872-878, 2018.

[7] T. Lin, H. Li and S. Yin, "Modified pyramid dual tree direction filter-based image de-noising via curvature scale and non-local mean multi-grade remnant multi-grade remnant filter," *International Journal of Communication Systems*, vol. 31, no. 16, 2018.

[8] J. Liu, S. L. Yin, H. Li and L. Teng, "A density-based clustering method for K-anonymity privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 12-18, Jan. 2017.

[9] Z. X. Lu, "Research and improvement of pageRank sort algorithm based on retrieval results," in *International Conference on Intelligent Computation Technology & Automation*, 2015. DOI: 10.1109/ICICTA.2014.119.

[10] X. Lu, J. Wang, L. Xiang, *et al.*, "An adaptive weight method for image retrieval based multi-feature fusion," *Entropy*, vol. 20, no. 8, 2018.

[11] L. Teng, H. Li, "A high-efficiency discrete logarithm-based multi-proxy blind signature scheme," *International Journal of Network Security*, vol. 20, no. 6, pp. 1200-1205, 2018.

[12] L. Teng, H. Li, "CSDK: A Chi-square distribution-kernel method for image de-noising under the IoT big data environment," *International Journal of Distributed Sensor Networks*, vol. 15, no. 5, 2019.

[13] S. Wang, K. Yan, X. Liang, "Quantitative interferometric microscopy with two dimensional Hilbert transform based phase retrieval method," *Optics Communications*, vol. 383, pp. 537-544, 2017.

[14] Y. Xu, L. Lin, H. Hu, *et al.*, "Texture-specific bag of visual words model and spatial cone matching-based method for the retrieval of focal liver lesions using multiphase contrast-enhanced CT images," *International Journal of Computer Assisted Radiology & Surgery*, vol. 13, no. 10, pp. 1-14, 2017.

[15] X. Yang, Y. Xun, S. Nepal, *et al.*, "A secure verifiable ranked choice online voting system based on homomorphic encryption," *IEEE Access*, vol. 6, no. 99, pp. 20506-20519, 2018.

[16] S. Yin, H. Li and J. Liu, "A new provable secure certificateless aggregate signcryption scheme," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1274-1281, Nov. 2016.

[17] S. L. Yin and J. Liu, "A K-means approach for map-reduce model and social network privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1215-1221, 2016.

[18] C. Zhang, X. Wang, J. Feng, *et al.*, "A car-face region-based image retrieval method with attention of SIFT features," *Multimedia Tools & Applications*, vol. 76, no. 8, pp. 1-20, 2017.

[19] L. Zou, X. Wang, S. Yin, "A data sorting and searching scheme based on distributed asymmetric searchable encryption," *International Journal of Network Security*, vol. 20, no. 3, pp. 502-508, 2018.

Biography

Xiaowei Wang biography. She is a full professor of the software college at Shenyang Normal University. Her interests are wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Prof. Wang had published more than 10 international journal and international conference papers on the above research fields. Email:hsiaoweiw@163.com.

Shoulin Yin biography. He received the B.Eng. and M.Eng. degree from Shenyang Normal University, Shenyang, Liaoning province, China in 2016 and 2013 respectively. Now, he is a Doctor in Harbin Institute of Technology. His research interests include Multimedia Security, Network Security, Filter Algorithm, image processing and Data Mining. Email:352720214@qq.com.

Hang Li biography. He obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hang Li is a full professor of the software college at Shenyang Normal University. His interests are wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Prof. Li had published more than 30 international journal and international conference papers on the above research fields. Email:lihangsoft@163.com.

Lin Teng biography. She now is taking the B.Eng. degree from Shenyang Normal University, Shenyang, Liaoning province, China in 2016. Also, she is a laboratory assistant in Software College, Shenyang Normal University. Her research interests include Multimedia Security, Network Security, Filter Algorithm and Data Mining. Email:910675024@qq.com.

Shahid Karim biography. Shahid Karim received his BS degree in electronics from Comsats Institute of Information Technology, Abbottabad, Pakistan, and his MS degree in electronics and information engineering from Xi'an Jiaotong University, China, in 2010 and 2015, respectively. He received his PhD at the Department of Information and Communication Engineering, School of Electronics and Information Engineering, Harbin Institute of Technology (HIT), China. Now, he is an Assistant associate professor in Department of Computer Science, ILMA University. His current research interests include image processing, object detection, and classification toward remote sensing imagery. Email: shahidhit@yahoo.com.