J Supercomput (2015) 71:3353–3372
DOI 10.1007/s11227-015-1413-0

A game theory-based block image compression method in encryption domain

Shaohui Liu[1] · **Anand Paul**[2] · **Guochao Zhang**[1] ·
Gwanggil Jeon[3]

Published online: 1 April 2015

Abstract With the development of digital imaging technology and the prevalence of mobile devices with camera, internet privacy has been a growing concern for public. Especially in some private chat groups in social network, for example, Facebook, WeChat, and MySpace, some people want to share their personal images by internet service provider without leaking this information while the internet service provider can also take some additional measures on these images, for example, reducing the network bandwidth. How to provide technologies or software with such functionalities, usually conflicting goals, becomes increasingly urgent in both academia and industry. Image encryption is a choice; however, it does not provide the additional function needed by internet service providers. Recently, game theory is widely used in network security to solve such problem with conflicting goals. In fact, there is a game theory between users and service providers. This paper proposes a block-based

✉ Shaohui Liu
shliu@hit.edu.cn; hitliushaohui@gmail.com

Anand Paul
anand@knu.ac.kr

Guochao Zhang
gczhang@hit.edu.cn

Gwanggil Jeon
gjeon@incheon.ac.kr

[1] School of Computer Science and Technology, Harbin Institute of Technology,
Harbin 150001, China

[2] School of Computer Science and Engineering, Kyungpook National University,
Taegu, South Korea

[3] Department of Embedded Systems Engineering, College of Information and Technology,
Incheon National University, Incheon, South Korea

image compression method in encrypted domain which provides not only the privacy protection capability but also the additional operation capability needed by internet service providers. This block-based method can be formulated as a game theoretical problem and can be optimized by game theory. First, the image to be shared will be encrypted in block-by-block way by owner with simple encryption operation. Second, the service providers can send the part or full of the encrypted image stream according to the available bandwidth with an adaptive parameter sets. Finally, the intended receivers can decrypt the received encrypted stream to recover the image. Extensive experiments show that the proposed algorithm improves the compression performance compared with the-state-of algorithms.

Keywords Image compression in encrypted domain · Image encryption · Privacy protection · Game theory · Network content security

1 Introduction

A great demand on developing models and methods for providing privacy protection and network communication security is growingly urgent in this digital era, where most of the digital information will be transmitted over different network and can be intercepted easily or leaked deliberately. In this paper, image and video are our concerns. With the growing popularity of mobile devices with micro cameras in recent decades, images and videos can be easily produced and then spread quickly through ubiquitous networks and have become a popular communication way in many social network service providers, such as Facebook, Wexin [1], Twitter, QQ, LinkedIn and so on. For example, according to the statistics in [2] posted at May 2014, Web and application users are sharing and uploading 1.8 billion photos a day. These platforms or service providers are providing novel opportunities for interaction among their users. People from all over the world can communicate, date, find jobs, share images and videos. While during this procedure, people are facing the risk of revealing the related personal privacy or sensitive information to strangers or service providers. In fact, there have been a few related issues, the latest one is that many private photos are leaked from the Apple's iCloud [3]. Of course, there are some other problems, for example video copy detection [4]. But in this paper, privacy is our focus. Besides, Web 2.0 applications also allow some new ways to link personal information [5]. For example, many service providers, such as Facebook and QQ, can apply facial recognition techniques to images uploaded by users to link their private or personal information of the identified persons [6]. Moreover, compared to text, image and video obviously place many more requirements on network bandwidth and media storage capacity. Although network bandwidth and storage space have been continuously increasing, the required storage space and corresponding running costs are exponential in growth [7]. Hence, encryption for security and compression for low bandwidth are hot topics in research community.

It is growing tendency that Internet networks are becoming more and more dependent on the interactions of intelligent devices that are capable of autonomously operating within a highly dynamic and rapidly changing environment. Many exist-

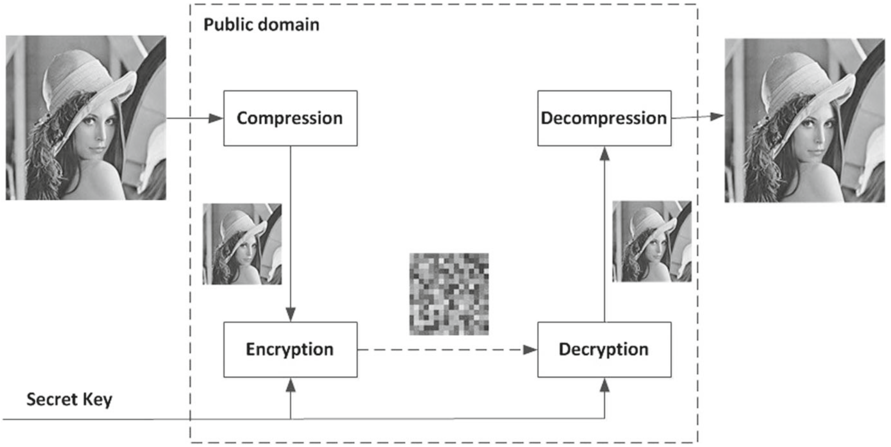


Fig. 1 Framework of general combination of compression and encryption

ing algorithms are needed to modify to adapt the development. Game theory provides the ideal framework for this [8] and network security [9]. For example, [10] gave a fairly comprehensive works which applied the game theory to address different forms of security and privacy problems in computer networks and mobile applications. And authors reviewed various game-theoretical formulations of network security issues. The interactions between an attacker and the administrator were modeled as a two-player stochastic game in [11]. In this paper, a game theory is used to formalize the image compression problem in encryption domain which an image first is encrypted and then is compressed.

In general, the framework of combination of image compression and encryption is illustrated as Fig. 1. Namely compression and encryption are independent operations in general applications. Once an image has been encrypted, then it is very hard to process this encrypted image because the statistics characteristic of the image has been interrupted by encryption. Hence, most of the techniques proposed so far to deal with image security try to apply some cryptographic primitives on the compressed image. The common case is partial encryption [12], where an encryption algorithm is used to encrypt only part of the compressed image or video to avoid the huge amount of operations because of the low speed of the encryption algorithm. From Fig. 1, plain image and encrypted image exist simultaneously in the public domain. In this paper, the public domain means that all data in this domain can be accessed by parties. Users do not control the transferred data. Obviously, it faces the risk of leakage of private information. Hence, one would ask naturally: is it possible that the image is encrypted firstly and then is compressed?

In recent years, some pioneering works are proposed in signal processing in encrypted domain [13,14]. Sometimes, it is called secure signal processing, which provides some solutions to this problem. In this paper, the signal processing is compression. Aiming at improving the compression performance and providing the capability of privacy protection, this paper extends the conference paper within the game theory [15] so that some potential powerful techniques can be used in this framework. In addition, it also proposes a novel block-based compression method with an automatic selective mechanism of parameters in encryption domain and conducts some extensive experiments. Our contributions are summarized as follows:

- A novel block-based compression method in encrypted domain is proposed. This block-based framework can provide some flexibility to deal with each block separately.
- This block-based compression method is formulated as a game theoretical problem. Where each block is a player in the game and the strategy of a player is how to allocate bits for that block. Moreover, this can be configured as a bargaining game.
- The type of the image and the smoothness of corresponding blocks are considered to improve the performance of proposed algorithm. These two factors then used to select the appropriate parameters to optimize the compression performance; concurrently, a partial random sampling restoration method is used to provide a better side information(SI) for recovering the original image.

The remainder of this paper is organized as follows. Section 2 presents the related works. In Sect. 3, firstly the block-based framework is formalized as a game theoretical problem and then an approximation solution, namely an adaptive parameter selection mechanism, is proposed. Extensive experimental results and discussions are reported in Sect. 4. At last, the conclusions are given in Sect. 5.

2 Related work

In the last decades, the rapid development of social network, online applications, cloud computing and distributed processing has aroused the concerns about to end-to-end security [16,17]. People want to share and exchange securely their images in social network service platform. Although they do not expect their contents being leaked even being exposed to service provider, there are at least two potential security risks where one is the channel provider, and the other is the platform provider. Traditionally, textual data can use encryption to achieve the objective. However, end-to-end security of multimedia data is not so easy like text data because of its huge amount of data. In addition, the channel providers also want to make full use of the bandwidth to maximize their profits. Thus, they have more interest in data compression while users are more concerned with image security. It seems that there is a trade-off between users and channel providers. Then, how to achieve this trade-off? The framework shown in Fig. 2 provides a potential solution; the difference from Fig. 1 is that images in the public domain are encrypted. It is obvious that the security in this framework is improved greatly. Following, some related work will be introduced.

Zhou et al. [18] proposed an image encryption algorithm based on discrete parametric cosine transform (DPCT), where the combination of the parameters of the DPCT and inverse DPCT provided the security. And Podesser et al. [19] and Yekkala et al. [20] proposed some algorithm using bitplane encryption to achieve secure transmission of image data in mobile environments. Although Zhou's method can be used in compressing procedure, these methods did not consider truly the compression. Is it possible to compress the encrypted data to lower the band-width?

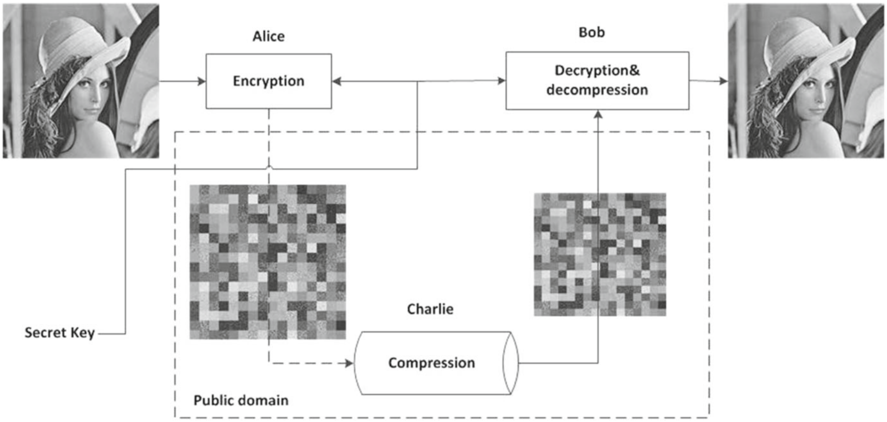


Fig. 2 Framework of combination of encryption and then compression

To compress the encrypted data in this scenario, Johnson et al. [14] proposed to use the theory of source coding to compress the encrypted data and they proved that the performance of compressing encrypted data can be as good as that of compressing non-encrypted data in theory. Partially, the work of Xiong et al. [21] has some similar considerations based on distributed source coding (DSC). Afterwards, Schonberg et al. [22] proposed to utilize Low density parity check (LDPC) codes to compress the encrypted data for memoryless and hidden Markov sources, where an incremental scheme based on exponentially increasing block lengths was proposed to balance the resolution rate of parameter estimation with the redundancy rate of communication. Then, they extended the statistical models to video to compress the encrypted video in [23]. Different from Schonberg's work, Barni et al. [24] proposed several methods to compress the encrypted images by employing LDPC codes into different bit planes. Because all of these methods are the lossless compression, the compression performance is very limited.

To improve the performance of compression in encryption domain, lossy compressing encrypted images have been developed. For example, in [25], the authors introduced the compressive sensing (CS) mechanism to compress the encrypted images, and a basis pursuit algorithm is used to enable joint decompression and decryption. Zeng et al. [26] proposed a resolution progressive compression algorithm which compressed an encrypted image progressively in resolution. In their method, the encoder sent a downsampled ciphertext image; once the decoder received this then reconstruct a low-resolution image, then intra-frame prediction was used to provide side information to improve the resolution to achieve the resolution progressive compression. This method achieves a much more efficient compression than existing algorithms. In addition, Kang et al. [27,28] proposed a compression scheme on pixel encrypted images.

Recently, Zhang [29] proposed a novel idea to compress the encrypted image using coset code and the iteratively reconstruction, where the original image was encrypted in the simple way of permuting the pixels positions, namely the position relationship was changed while the pixels' value were kept unchanged. Then, a transform was also applied to some elastic pixels to reduce the bits to be transmitted based on coset code theory. The compression performance and the quality of the constructed result are both much better than those of the previous methods due to using the iteratively reconstruction technique. However, the performance obtained is based on the whole image. According to the theory of coset code, the quantization step and the quality of side information are very important parameters to the reconstructed result. In fact, the nearest neighbor estimation (NNE) in [29] to get the SI is far away the optimal case. Moreover, the quantization step in transform coding in [29] is fixed and it cannot be determined automatically. Inspired by the work in [29], we propose an improved block-based compression method in encrypted domain. It is well known that different regions in image have different characteristics. Hence, it is more reasonable method that different compression parameters are used in compression side according to the local statistics. In this paper, an adaptive quantization step choosing strategy is proposed and Image Restoration from partial random samples (IRPRS) [30] is used to generate the more exact SI.

At the block level, the problem can be formulated as a game theoretic problem. In fact, the parameter sets in each block can affect the number of compressed bitstream of that block. Thus, each block competes for a share of resources, which are the target compression ratio of the image. Based on Nash bargaining solution (NBS) [8,31], a cooperative game is used to formalize the problem.

3 Block-based image compression in encrypted domain

Actually, signal processing in encryption domain has attracted attentions of many researchers due to the privacy protection capability incurred by the processing in encryption domain. The image compression in encryption domain (ICED) is a specific application. Just like the traditional compression scenario, ICED also expects to use as possible as smaller bits while maintaining high quality. In other words, when the bits allocated for the image have been fixed, one tries his best to improve the quality of decompressed image. It is well known that people are more sensitive to subjective quality than objective quality for images. Hence, in this paper, a block-based ICED is proposed to make a trade-off between bit allocation in different blocks. This block-based method masks the imperceptible distortion and improves the perceptual quality using a game theory method providing optimality and fairness of bit allocation. This is a inherent merit of block-based method. Following, the encryption, compression, decompression and image reconstruction will be introduced separately.

3.1 Image encryption and decryption

Encryption is a key measure to provide privacy protection in digital era. Compared with text encryption, multimedia encryption often uses partial encryption to avoid huge operations of multimedia. Image encryption in spatial domain can be classified into three categories: position permutation, value transformation, and visual encryption which are widely used to share images. In the proposed scheme, a hierarchical encryption is proposed to encrypt the image to effectively and efficiently compress the

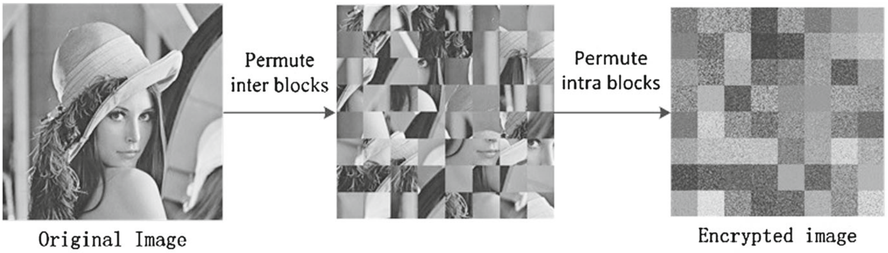


Fig. 3 An illustration of hierarchical encryption

encrypted image. First, the permutation encryption is utilized to permute the image blocks and then each block is also permuted by position. An illustration is shown in Fig. 3. The detailed process is given below.

1. Dividing the image into n blocks with the same size (e.g., 32×32);
2. Permuting the position of all blocks by a key occurred by a key derivation function (KDF);
3. Permuting the pixels in each blocks by keys which are also generated by KDF, it is noted that this block partition and KDF mechanism do not sacrifice the security remarkably.

Only the secret key seed is sent to the decoder to decrypt the image. One inter-block secret key and n intra-block secret keys can be generated with the same key generation mechanism as the encoder and the decryption is similar as encryption above.

3.2 Compression of encrypted image

As mentioned earlier, Zhang's method [29] does not provide the optimal parameters. Once the α is fixed, then all the remaining procedures are fixed, and the performance will be determined. However, this does not meet the real applications. For example, the service providers want to transmit adaptively appropriate bits according to the available network bandwidth, namely they expect that the α varies with the available bandwidth. Another example is how to allocate optimal bits for different blocks when the available network bandwidth is fixed to maximize the quality of reconstruction image. In this proposed block-based method, block-level bit allocation can be formulated as a game theoretical problem in game theory, where each block is regarded as a player in the game. N players compete for the use of bits to maximize the perceptual quality of reconstructed image. Of course, this can be extended to the video compression in encrypted domain just like what is mentioned in the reference [31]. The diagram of encoder is shown in Fig. 4.

3.2.1 The bargaining game configuration of block-based framework

In the proposed block-based compression framework, there is a trade-off between the compression efficiency and image quality. It is obviously that more bits will lead

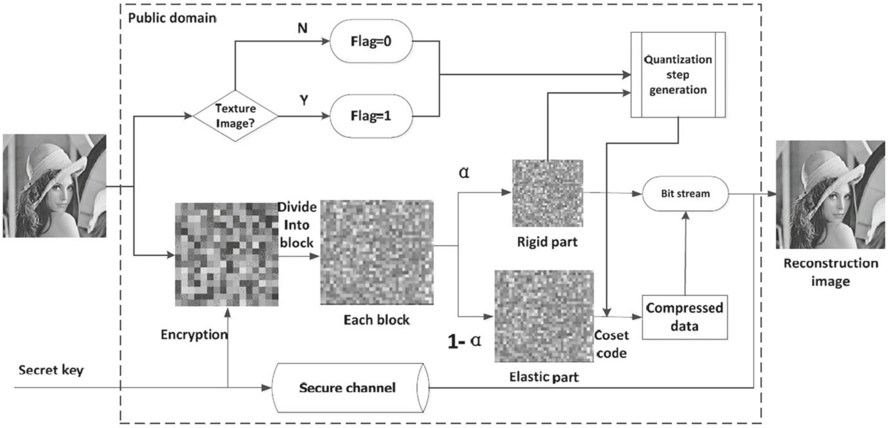


Fig. 4 Framework of proposed block-based compression in encryption domain

to higher quality. In [29], it is difficult to model the optimal strategy because the image is looked as a whole unit. Actually, even the target bits are determined, we still can improve the algorithm to optimize the performance. Game theory provides mathematical tools and models for this type of problem. In this paper, game theory is used to investigate the trade-off relationship between quality and desired bits. In this scenario, every block B_i has an incentive to optimize its representation so as to maximize the quality of decompressed and reconstructed block. It should be noted that the reconstruction and recovery have the same meaning in this context without explicit explanation. This optimization will lead to a more preferable visual quality for the block B_i with some sophisticated techniques, thus requiring B_i to be represented effectively and efficiently. And the bargaining game is configured as follows.

Players Each image can be partitioned into N blocks. Each block is regarded as a player in the game. These N players compete for the use of a fixed resource to achieve the destination, which is the target image quality under the fixed compression ratio for the image.

Strategies The strategy of a player is how to control the number of bits which is used to represent the compressed stream under the condition of maximizing the quality of the reconstructed image. Suppose the original bits for the image be T and the fixed compression ratio is R, each block's bits for representing the compressed bitstream is t_i. Then, the maximum permitted number of bits for the compressed image is $T \times R$; the total bits requested by the N blocks should be no more than $T \times R$. It can be formulated as:

$$\sum_{i=1}^{N} t_i \leq T \times R. \tag{1}$$

Utility A utility function for each block is the quality of reconstructed block. Higher quality under some fixed compression ratio is more preferable. Given a combination of strategies carried out by all blocks (it should be noted that the strategies are determined by parameter sets P), then the utility of the game can be represented as $u = (u_1(B_1, P_1), u_2(B_2, P_2), \ldots, u_N(B_N, P_N))$, where the utility is a function of each block B_i and corresponding parameter sets P_i.

Initial utility The initial utility of the block can be determined by setting all blocks with the same parameter sets; this is just the case described in [29]. Thus, the initial utility of the game u^0 is defined as $u^0 = (u_1^0(B_1, P_1^0), u_2^0(B_2, P_2^0), \ldots, u_N^0(B_N, P_N^0))$, where $P_1^0 = P_2^0 = \cdots = P_N^0$.

According to the game theory [8], NBS is a unique solution that satisfies a set of axioms for fair bargain. Therefore, to find the NBS, we need to solve the following maximization problem:

$$\max \prod_{i=1}^{N} (u_i(B_i, P_i) - u_1^0(B_i, P_i^0)) \ \text{ s.t.} \sum_{i=1}^{N} t_i \leq T \times R. \tag{2}$$

where t_i depends on B_i and P_i. This inequality constrained optimization problem can be solved by Lagrangian multiplier method [31]. In this paper, an approximation processing in which P_i is tuned according to the type of B_i is introduced in next subsection.

3.2.2 Block-based compression

The encrypted image is compressed block by block according to the following steps. Each block is processed as similar as in reference [29]. From the Fig. 4, the main differences include block mechanism, the parameter selection and IRPRS initialization. The first two parts are the key parts in Eq. 2. Actually, P_i in this approximated processing includes α and Δ, and the initial value of α is 0.25 in Subsect. 4.1.

1. The encrypted block will be divided into two parts : rigid part and elastic part. Each encrypted block can be treated as a vector length of N, and $\alpha \times N$ pixels are selected randomly, namely $p_1, p_2, \ldots, p_{\alpha \cdot N}$. These pixels are reserved, therefore, its named rigid part as in [29]. While the rest part is denoted as $q_1, q_2, \ldots, q_{(1-\alpha)\cdot N}$ and its called elastic part because its redundancy will be reduced. The elastic part will be compressed.
2. Perform orthogonal transformation to the elastic part with a public orthogonal matrix H and denote the transformation coefficients as $Q_1, Q_2, \ldots, Q_{(1-\alpha)\times N}$. The detailed procedure is shown in (3):

$$[Q_1, Q_1, \ldots, Q_{(1-\alpha)\times N}] = [q_1, q_1, \ldots, q_{(1-\alpha)\times N}] \times H. \tag{3}$$

3. For each Q_k calculate:

$$s_k = \text{mod}\left[\text{round}\left(\frac{Q_k}{\Delta}, M\right), M\right], \quad k = 1, 2, \ldots, (1-\alpha)N \tag{4}$$

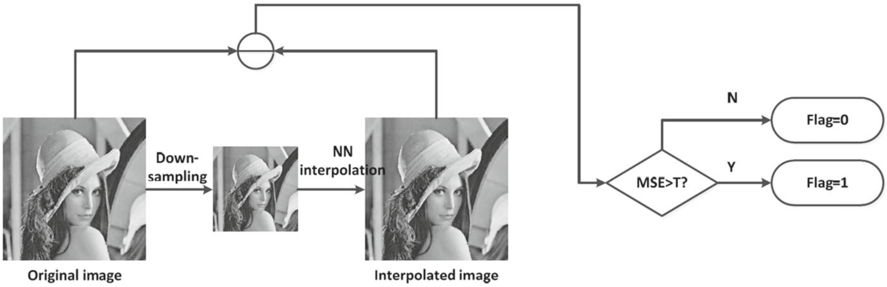


Fig. 5 An illustration of how to determine the type of an image

where Δ and M are system parameters. The mod operation returns the remainder and the round operation gets the nearest integer. It is obviously that s_k belongs to $[0, M-1]$ from (4). The smaller the M, the less is the amount of elastic part pixel.

Q_k can be rewritten as the following way:

$$Q_k = r_k \cdot \Delta + s_k \cdot \frac{\Delta}{M} + t_k,$$

where r_k and s_k are integers. Obviously, s_k in $[0, M-1]$, $t_k \in \left[-\frac{V}{2 \cdot M}, \frac{V}{2 \cdot M}\right]$.

Here, the compression ratio R can be calculated as:

$$R = \frac{8 \cdot \alpha \cdot N + \log_2 M \cdot (1-\alpha) \cdot N}{8 \cdot N} = \alpha + (1-\alpha) \cdot \frac{\log_2 M}{8}. \tag{5}$$

3.2.3 Adaptive selection of parameters

The smoothness of an image has a dramatic effect on the quality of SI in the decoder side, and different type content of an image has a different effect on the perceptual quality. Thus, the perceptual quality of reconstructed image will be enhanced remarkably if the types of images and blocks are considered to design the compression algorithm. But after encryption has been applied, the discrimination is very difficult. Therefore, this paper proposes a method to differentiate the type of images and blocks in sender side. Considering the processing of reconstruction, a nearest neighbour interpolation is used to recover the down-sampling image to calculate the MSE which is used to determine the type of images. The procedure is illustrated as in Fig. 5.

Once the image type has been determined, then the parameters Δ and α of each block can also be selected adaptively. According to the coset code theory, when the quality of SI is high, the less quantization step can provide better results. Experiments also indicate that this analysis is reasonable. In addition, even the smooth block has a smaller α, the algorithm still obtains a good SI. For α, a slight adjustment is used according to the smoothness of each block. To simulate the relation between the best quantization step and the corresponding block rigid part's variance, we train some images and give a fitting function, where the rigid part of ith block as rigid_i, and x, the variance of rigid_i, is as a measure of the degree of smoothness of this block.

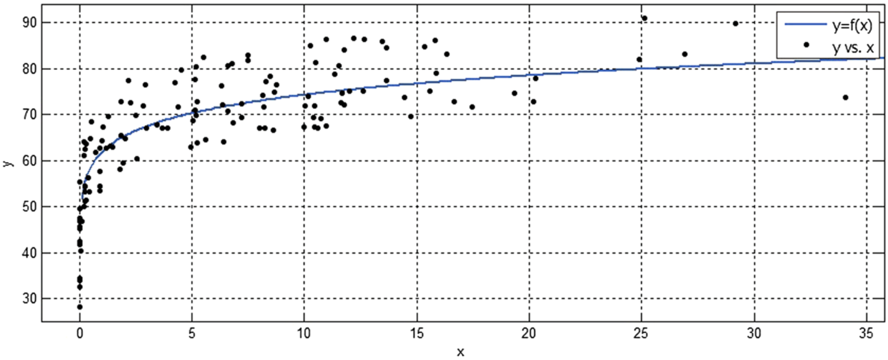


Fig. 6 The fitting curve between the variance and quantization step in non-texture images

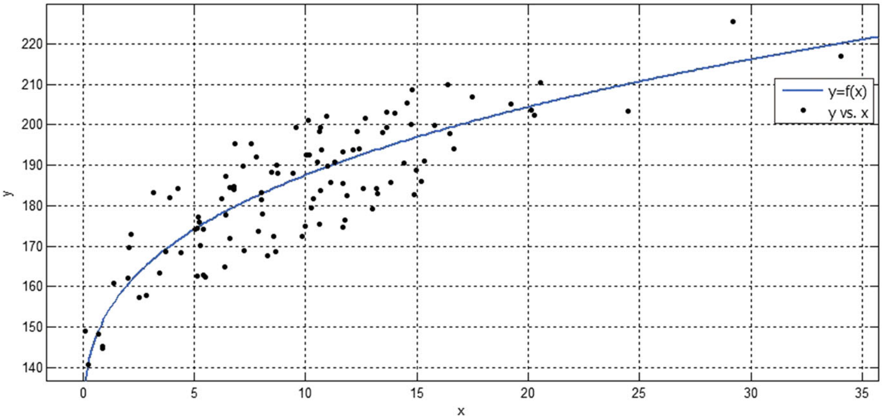


Fig. 7 The fitting curve between the variance and quantization step in texture images

$$f(x) = ax^b + c, \tag{6}$$

where $f(x)$ is the best quantization step, and the fitting result is shown in Figs. 6 and 7.

3.3 The processing of reconstruction

At the decoder, the received data stream includes: secret key seed, system parameters, a series of rigid pixels and the corresponding s_k. The SI is then used to assist the reconstruction. This paper proposes an improved method to generate SI, that is, IRPRS method. The reconstruction framework is shown in Fig. 8.

In the process of SI generation, all methods use the prior knowledge of the image. Actually, there are two kinds of prior knowledge, namely, local smoothness and non-local self-similarity[30]. In reference [29], the NNE method is used to generate the SI; this priori knowledge is mainly based on local smoothness. The IRPRS method which incorporates local smoothness and non-local self-similarity priori knowledge

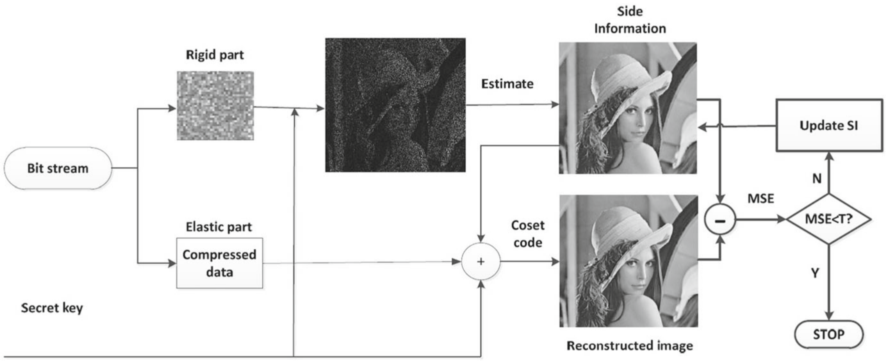


Fig. 8 Framework of proposed decompression and recovery method

is used to generate the SI. The specific reconstruction is described as follows and is similar as described in [29].

1. Put the rigid pixels in the right place with the secret key;
2. Estimate the elastic pixels with IRPRS and denote as $q'_1, q'_2, \ldots, q'_{(1-\alpha)N}$;
3. Calculate the coefficients

$$[Q'_1, Q'_2, \ldots, Q'_{(1-\alpha)N}] = q'_1, q'_2, \ldots, q'_{(1-\alpha)N} \cdot H$$

and

$$s'_k = \mathrm{mod}\left(\frac{Q'_k}{\Delta} \cdot M, M\right).$$

Denote the difference between s'_k and s_k as d_k. That is $d_k = s'_k - s_k, k = 1, 2, \ldots, (1-\alpha) \cdot N$;

4. Update Q'_k according to d_k as follows

$$Q''_k = \begin{cases} \left(\lfloor \frac{Q'_k}{\Delta} \rfloor + 1\right) \cdot \Delta + s_k \cdot \frac{\Delta}{M}, & \text{if } d_k \geq \frac{M}{2} \\ \lfloor \frac{Q'_k}{\Delta} \rfloor \cdot \Delta + s_k \cdot \frac{\Delta}{M}, & \text{if } -\frac{M}{2} \leq d_k < \frac{M}{2} \\ \left(\lfloor \frac{Q'_k}{\Delta} \rfloor - 1\right) \cdot \Delta + s_k \cdot \frac{\Delta}{M}, & \text{if } d_k < \frac{M}{2} \end{cases} \tag{7}$$

Then, perform the inverse transformation to Q''_k:

$$[q''_1, q''_2, \ldots, q''_{(1-\alpha)N}] = [Q''_1, Q''_2, \ldots, Q''_{(1-\alpha)N}] \cdot H^{-1}. \tag{8}$$

Finally, calculate the average value of difference between $q_k^{'}$ and $q_k^{''}$,

$$D = \frac{1}{(1-\alpha)\cdot N} \cdot \sum_{k=1}^{(1-\alpha)N} (q_k^{''} - q_k^{'})^2 \tag{9}$$

If D is not less than the threshold T, for each elastic pixel, calculate the average value of its four neighbor pixels (e.g., up, down, left and right) as its new estimated value, then go to step 3. Otherwise, the rigid pixels and the latest elastic pixels are combined as the final reconstructed result.

4 The experimental results and analysis

To evaluate the performance of the proposed method, we compare it with Zhang's method. Totally, eleven images from the USC-SIPI image database [32] are used in this section, where six non-texture images include House (gray 256 × 256), Lena(gray 512 × 512), Pepper (gray 512 × 512), Boat (gray 512 × 512), Airplane (gray 512 × 512), Girl ($gray$256 × 256), and five texture images include Baboon (gray 512 × 512), Grass (gray 512 × 512), Bark (gray 512 × 512), Straw (gray 512 × 512), Pressed calf leather (gray 512 × 512).

4.1 System parameters and settings

In Zhang's paper, M is the base and α is fixed to set the ratio of preserved rigid pixels. The set of {4,6,8} is used for testing the performance in Zhang's paper. Thus, we use the same set for M. As for, it is only an initial value in our proposed method, and then the algorithm will adjust this parameter adaptively. The two methods are compared with the same M and $M \in \{4, 6, 8\}$, $\alpha = 0.25$. In Zhang's method, it did not propose how to choose the step Δ. We draw the conclusion that the optimal set of Δ is {80, 100, 120} for non-texture image, and the optimal set is {180, 200, 220} for non-texture image through extensive experiments. Thus, these two optimal sets of step parameters are used in this section. In the experiments, our comparison results are done under the same compression ratio. Thus, these settings do not affect the experiments.

Compared with Zhang's method, the proposed method uses the selected parameters described in Sect. 3.2. Moreover, to evaluate the effect of SI on performance, the two different methods to generate the side information are also investigated: One is proposed in [29] called NNE (denoted as $\text{Block}_{\text{NNE}}$ for convenience), the other is IRPRS (denoted as $\text{Block}_{\text{IRPRS}}$ for convenience).

4.2 Experimental results

Although the proposed method increases the complexity a bit, the reconstructed results are improved greatly and the cost is acceptable. The results of experiments on non-texture images are shown in Figs. 9 and 10 under different compression rates and those

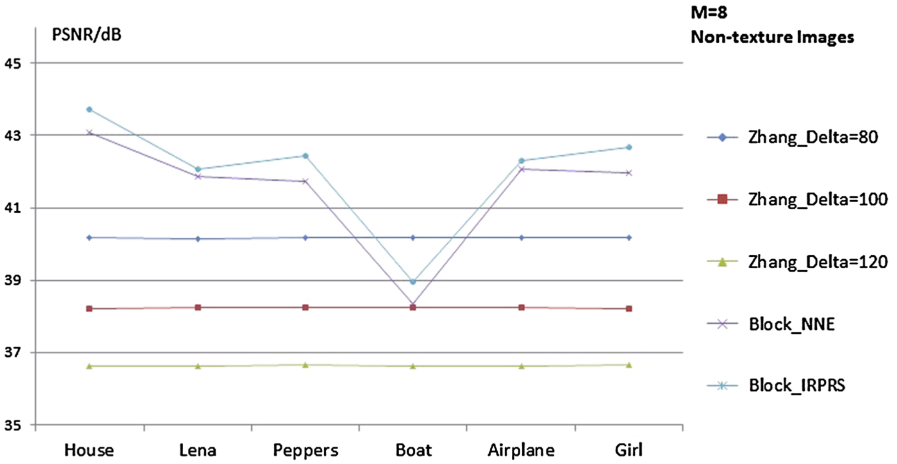


Fig. 9 Performance comparison of proposed methods and Zhangs method while the compression ratio R is 0.53 on non-texture images

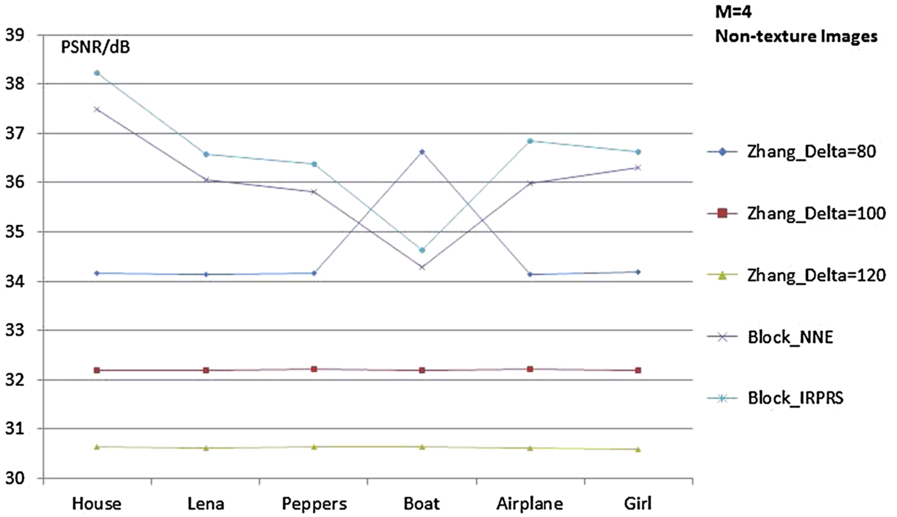


Fig. 10 Performance comparison of proposed methods and Zhangs method while the compression ratio R is 0.43 on non-texture images

results on texture images are shown in Figs. 11 and 12. The graph presented in the Figs. 9 and 10 shows that the Block$_{\mathrm{NNE}}$ method obtains better results than Zhang's method (it is noted that the best three Deltas are chosen) except the Boat image. For texture images, the Block$_{\mathrm{NNE}}$ method outperforms the Zhang's method in all images. Moreover, the Block$_{\mathrm{IRPRS}}$ gets slightly better results than the Block$_{\mathrm{NNE}}$ because the first method can get the better initialization. Although the iterative reconstruction is the same as Zhang's method except the initialization, the final result is not exactly same. The reason is that the IRPRS can exploit the local smoothness and non-local

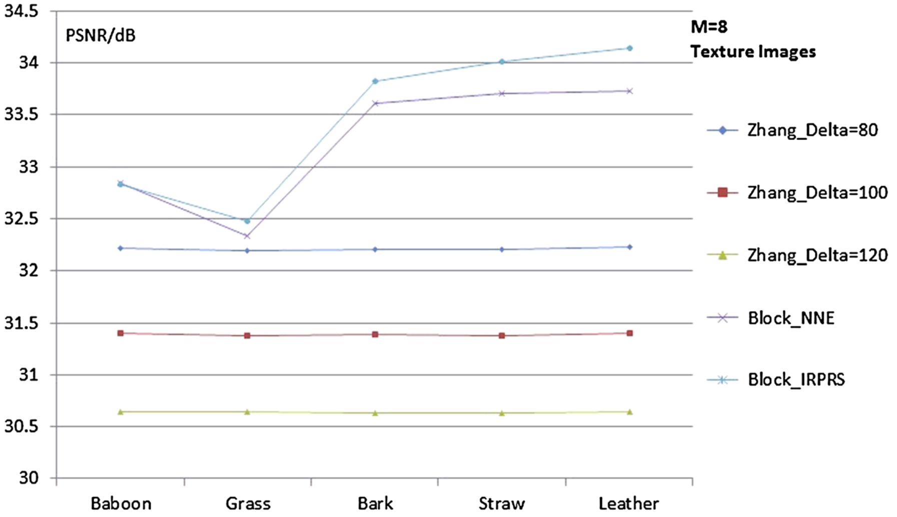


Fig. 11 Performance comparison of proposed methods and Zhangs method while the compression ratio R is 0.53 on texture images

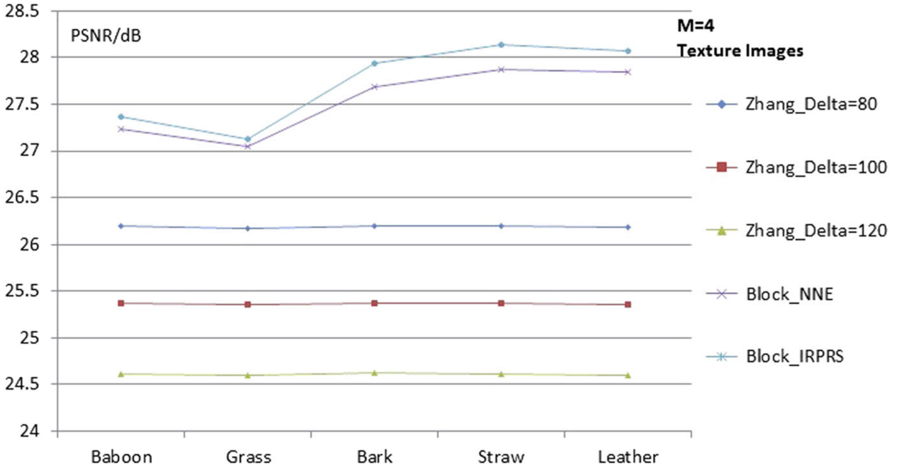


Fig. 12 Performance comparison of proposed methods and Zhangs method while the compression ratio R is 0.43 on texture images

self-similarity fully. In addition, the average gain for texture images is much larger than one for non-texture images; the reason is the texture images have complex texture so that they will cost more bits to code the same amount information.

The specific numerical results are shown in Table 1, where the second column indicates the type of image, namely texture or non-texture images. For convenience, Y denotes texture images, and N denotes non-texture images. The experiment results show that the proposed Block$_{\text{NNE}}$ obtains gains from 1.15 dB to 2.99 dB compared with Zhang's method on average for all images under different compression ratios. The

Table 1 Comparison of proposed methods with Zhang's method in PSNR (db)

Ratio		Zhang	Block$_{\mathrm{NNE}}$	Gain	Block$_{\mathrm{IRPRS}}$	Gain
0.53	N	48.94	42.31	2.12	42.69	0.38
0.53	Y	32.22	33.37	1.15	33.58	0.21
0.48	N	37.68	39.97	2.29	40.40	0.43
0.48	Y	29.74	31.05	1.31	31.22	0.17
0.43	N	34.18	36.47	2.29	37.05	0.58
0.43	Y	24.63	27.62	2.99	27.79	0.17

Table 2 Comparison of SSIM

Ratio		Zhang	Block$_{\mathrm{IRPRS}}$	Gain vs. Zhang
0.53	Non-texture	0.9717	0.9893	0.0176
0.53	Texture	0.9924	0.9947	0.0023
0.48	Non-texture	0.9524	0.9817	0.0293
0.48	Texture	0.9867	0.9910	0.0043
0.43	Non-texture	0.9051	0.9631	0.0580
0.43	Texture	0.9714	0.9804	0.0090

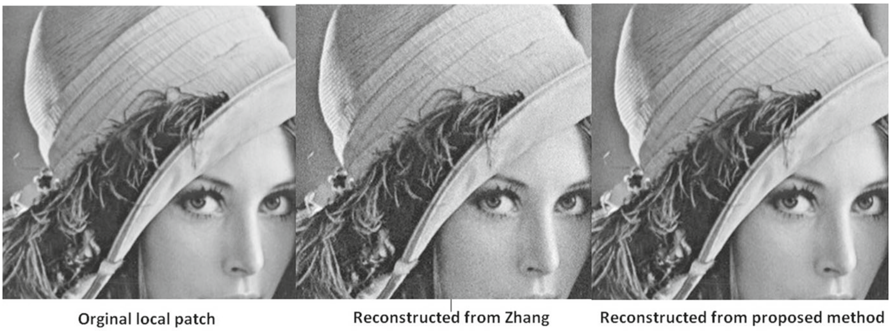
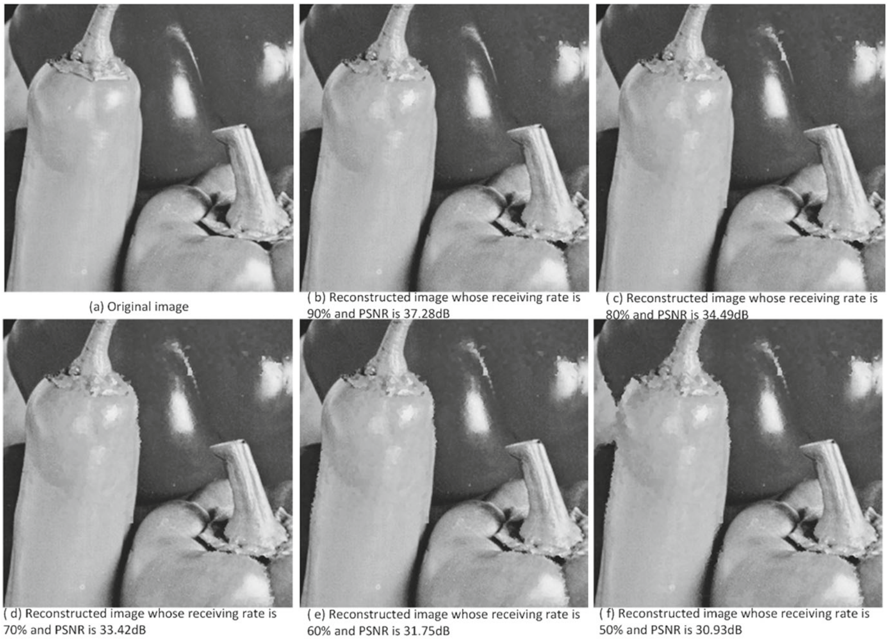


Fig. 13 Performance comparison of Block$_{\mathrm{IRPRS}}$ and Zhang's method while the compression ratio R is 0.43 on non-texture images

fifth column is the gain of Block$_{\mathrm{NNE}}$ against Zhang's method, and the seventh column is the gain of Block$_{\mathrm{IRPRS}}$ against Block$_{\mathrm{NNE}}$. Table 1 also indicates that the Block$_{\mathrm{NNE}}$ and Block$_{\mathrm{IRPRS}}$ can improve the performance. As mentioned earlier, Block$_{\mathrm{NNE}}$ and Block$_{\mathrm{IRPRS}}$ compress the image by the way of block-by-block to get a better perceptual quality. Here, the Structural SIMilarity (SSIM) index which is widely used in image quality evaluation [33] is used to measure the quality of compressed images. Results are shown in Table 2. From this result, a little gain is obtained, and the gain from non-texture images is larger than one from texture images. In addition, the proposed method's subjective quality of the reconstructed result is shown in Fig. 13 and the compression ratio is both 0.43.



(a) Original image

(b) Reconstructed image whose receiving rate is 90% and PSNR is 37.28dB

(c) Reconstructed image whose receiving rate is 80% and PSNR is 34.49dB

(d) Reconstructed image whose receiving rate is 70% and PSNR is 33.42dB

(e) Reconstructed image whose receiving rate is 60% and PSNR is 31.75dB

(f) Reconstructed image whose receiving rate is 50% and PSNR is 30.93dB

Fig. 14 Quality scalability of proposed method

The proposed block-based framework has a capability of scalability. If the rigid part bits can be totally received at the receiver side, the elastic parts can be partially received due to network issues. Then, the scalability of image quality can be still obtained. Figure 14 shows the results where the receiving rate is defined as the ratio of received elastic bits and total elastic bits.

4.3 Discussions

The performance in [29] exhibits excellent performance. In this paper, a block-based framework based on the work of [29] is proposed to improve the performance. This block-based framework can be directly extended to scalable quality reconstruction. Due to limited space, it is not introduced. Some discussions are given as follows.

4.3.1 Security

From the processes of encryption and compression [27–29], the encryption process is always relatively simple. As already mentioned above, compression is used to remove the redundancy which is from the encrypted image. Thus, the encryption operation does not make an image a true random image otherwise the compression cannot be performed. First the approximated image is restored by simple decryption, and then combining some additional information and a local model of an image such as bitplane correlation [24] or pixel correlation [28] are used as axillary information to improve the quality of the approximated image. Although there is a leakage of statistical information, the permutation-based encryption may be enough in most scenarios without a requirement of perfect secrecy just like partial encryption in image and video.

4.3.2 Compression performance

In this paper, the proposed block-based framework has some intrinsic advantages. It is similar to the block-based framework in many compression standards, for example JPEG, JPEG2000, H.264. Moreover, this is why so many standards use this block-based framework. However, this mechanism causes some block artifacts. Thus, some more accurate bit allocation methods and models are needed to deal with it. As earlier mentioned above, game theory may be a potential solution. Our method is an approximation to the Eq. 2, thus the final parameters are still too crude so that the improvement in performance is limited. In addition, another important factor affecting the performance is the mechanism to reconstruct the image. There are some choices such as NNE in [29], interpolation and prediction in [28], and IRPRS [30]. The key problems include how to construct the most appropriate image model and how to select adaptively an image model for some specific images.

4.3.3 Applications

Signal processing in encryption domain has many applications [13,34,35]. In many Web applications, client-to-client security is expected extensively [16]. However, image compression in encrypted domain is firstly proposed in [14] inspired by [21]. At that time, it does not have some very successful applications. Afterwards, Zeng et al. [26] proposed a typical application scenarios in sensor network where the sender Alice wants to send some private information to Bob while she wants to keep this private information be confidential to Charlie who is the network provider. Actually, ICED can be used in all places in which privacy protection is needed, for example, private images sharing among some close relationships. In fact, this proposed method can be easily extended to sharing scheme. Of course, the sender, service provider and receiver do not have to be different parts. Moreover, the sender does not have to be the part with limited resources.

More important, all these problems with conflicting parts can be formalized as a game theoretical problem, and then some optimization techniques can be used to solve those problems just like references [9–11,31].

5 Conclusions

This paper proposed a block-based image compression algorithm in the encryption domain. The compression problem is formalized as a game theoretical problem where the utility function is mainly based on block characteristic and its parameters sets. Due to the characteristics of the block-based framework, each block can choice adaptively the parameters to optimize the performance. Thus, an approximation solution for this game theoretical problem is proposed. First the type of an image is considered, and then the relationship between the degree of smoothness of each block and corresponding parameters is investigated to determine the most appropriate parameters. IRPRS method is used to generate the more accurate SI. The experimental results show that the proposed method can achieve a better reconstructed result compared with Zhang's method at the same compression ratio.

Acknowledgments This work was supported in part by the Major State Basic Research Development Program of China under Grant 2015CB351804, a scholarship from the China Scholarship Council of the Republic of China under Grant No. 201203070360 and the Natural Science Foundation of China under Grant No.60803147. The authors would like to thank the authors of [29,30] for kindly providing their source codes.

References

1. http://weixin.qq.com/
2. http://recode.net/2014/05/28/look-at-this-were-uploading-and-sharing-a-staggering-1-8-billion-photos-a-day/
3. Molina B (2014) Personal Apple: iCloud not breached in celebrity photo leak. Sep. 2014. online available: http://www.usatoday.com/story/tech/personal/2014/09/02/apple-icloud-leak/14979323/
4. Nie XS, Liu J, Sun JD, Wang LQ, Yang XH (2013) Robust video hashing based on representative-dispersive frames. Sci China Inform Sci 56(6):1–11
5. Squicciarini AC, Lin D, Sundareswaran S, Wede J (2014) Privacy policy inference of user-uploaded images on content sharing sites. IEEE Trans Knowl Data Eng. doi:10.1109/TKDE.2014.2320729
6. Mitchell J (2010) Making photo tagging easier. Online Available: http://blog.facebook.com/blog.php?post=467145887130
7. Gao W, Tian YH, Huang TJ, Yang Q (2010) Vlogging: a survey of videoblogging technology on the web. ACM Comput Surv 42(4): Article No.15
8. Zhu, H, Dusit N, Walid S, Tamer B (2012) Game theory in wireless and communication networks-theory, models and applications. Cambridge Uinversity Press, Cambridge
9. Roy S, Ellis C, Shiva S, Dasgupta D, Shandilya V, Wu QS (2010) A survey of game theory as applied to network security. In: Proceedings of the 43rd Hawaii international conference on system sciences, Honolulu, HI, pp 1–10
10. Mohammad H, Zhu QY, Tansu A, Tamer B, Hubaux JP (2013) Game theory meets network security and privacy. ACM Comput Surv 45(3): Article 24
11. Lye KW, Wing JM (2005) Game strategies in network security. Int J Inf Secur 4:71–86
12. Cheng H, Li XB (2000) Partial encryption of compressed images and videos. IEEE Trans Signal Process 48(8):2439–2451
13. Signal Guest editors: Piva A, Katzenbeisser S (2007) Processing in the encrypted domain. EURASIP J Inform Secur 2007
14. Johnson M, Ishwar P, Prabhakaran VM, Schonberg D, Ramchandran K (2004) On compressing encrypted data. IEEE Trans Signal Process 52(10): 2992–3006
15. Zhang GC, Liu SH, Jiang F, Zhao DB, Gao W (2013) An improved image compression scheme with an adaptive parameters set in encrypted domain. VCIP 2013:1–6
16. Hassinen M, Mussalo P (2005) Client controlled security for web applications. In: The 30th anniversary on local computer networks, IEEE Computer Society, pp 810–816
17. Poller A, Steinebach M, Liu H (2012) Robust image obfuscation for privacy protection in Web 2.0 applications. IS&T SPIE Electronic Imaging. In: International society for optics and photonics, SPIE, 830304-830304-15
18. Zhou Y, Panetta K, Agaian S (2009) Image encryption using discrete parametric cosine transform. In: Proceedings of the 43rd asilomar conference on signals, systems and computers, ser. Asilomar'09. Piscataway, NJ, USA. IEEE Press, pp 395–399
19. Podesser M, Schmidt HP, Uhl A (2002) Selective bitplane encryption for secure transmission of image data in mobile environments. In: The 5th nordic signal processing symposium, pp 10–37

20. Yekkala A, Madhavan CEV (2007) Bit plane encoding and encryption. In: Proceedings of the 2nd international conference on pattern recognition and machine intelligence, ser. PReMI'07. Springer, Berlin, pp 103–110
21. Xiong ZX, Liveris AD, Cheng S (2004) Distributed source coding for sensor networks. IEEE Signal Process Mag 21(5):80–94
22. Schonberg D, Draper SC, Ramchandran K (2005) On blind compression of encrypted correlated data approaching the source entropy rate. In: Proceedings of the 43rd Annual Allerton Conference, Allerton, IL
23. Schonberg D, Draper SC, Yeo CH, Ramchandran K (2008) Toward compression of encrypted images and video sequences. IEEE Trans Inform Forensics Secur 3(4):749–762
24. Lazzeretti R, Barni M (2008) Lossless compression of encrypted greylevel and color images. In: Proceedings of the 16th EUSIPCO, Lausanne, Switzerland
25. Kumar AA, Makur A (2009) Lossy compression of encrypted image by compressive sensing technique. TENCON 2009–2009 IEEE Region 10 Conference, pp 1–5
26. Liu W, Zeng W, Dong L, Yao Q (2010) Efficient compression of encrypted grayscale images. IEEE Trans Image Process 19(4):1097–1102
27. Kang XG, Xu XY, Peng AJ, Zeng WJ (2012) Scalable lossy compression for pixel-value encrypted images. In: IEEE data compression conference 2012, Snowbird, Utah, USA April 10–12
28. Kang XG, Peng AJ, Xu XY, Cao XC (2013) Performing scalable lossy compression on pixel encrypted images. EURASIP J Image Video Process 32:1–6
29. Zhang XP (2011) Lossy compression and iterative reconstruction for encrypted image. IEEE Trans Inform Forensics Secur 6(1):53–58
30. Zhang J, Xiong RQ, Ma SW, Zhao DB (2011) High-quality image restoration from partial random samples in spatial domain. In: IEEE visual communications and image processing (VCIP), pp 1–4
31. Ahmad I, Luo JC (2006) On using game theory to optimize the rate control in video coding. IEEE Trans CSVT 16(2):209–219
32. http://sipi.usc.edu/database/
33. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612
34. Lagendijk RL, Erkin Z, Barni M (2013) Encrypted signal processing for privacy protection: conveying the utility of homomorphic encryption and multiparty computation. IEEE Signal Process Mag 30(1):82–105
35. Yao Q, Zeng W, Liu W (2009) Multi-resolution based hybrid spatiotemporal compression of encrypted videos. In: Proceedings of the IEEE international conference on acoustics speech and signal processing, Taipei, Taiwan, ROC, 725–728