Secure Communication Scheme for Color Image Based on Index Technology

Jingyu Peng
Applied Technology College
Soochow University
Suzhou, China
kymiao@163.com

Yong Ren
Applied Technology College
Soochow University
Suzhou, China
renyong@suda.edu.cn

***Abstract*—A secure communication scheme for true color image was proposed. It is aimed at the hiding problem of a huge amount of true-color image data in the covert communication and maintaining the good visual quality of carrier image. Secure communication is achieved by combining encryption and hiding. Encryption on secret image is performed in the spatial domain of carrier image. Instead of changing pixel physics position or gray value, encryption method is searching the index value of secret image and hiding it in carrier image. Carrier image is designed as a palette, and the use of chaotic signal to act on the carrier image makes palette colors rich and evenly distributed. Each pixel of secret image is adaptively mapped to a subscript in palette by the minimum principle of Euclidean distance. Secret image is compressed and encoded as a data stream during encryption, reducing the amount of data to be hidden. Secret image is hidden in the wavelet domain of carrier image by using the lifting wavelet transform and multi-channel spread-spectrum embedded way. Simulation experiments show that this secure communication scheme reduces hidden data amount and improves information hiding transparency to ensure the concealment and safety of communication.**

Keywords-Secure communication; Image compression; Chaotic system; Index technology

I. INTRODUCTION

The rapid development of the Internet has provided more and more conveniences for people to pass information. However, information divulging and embezzlement also bring more and more insecurities. Therefore, information encryption technology has been research hotspot for years. A large amount and high correlation of data bring challenges to traditional password encryption technology and inconvenience to rapid information transmission and storage for color image. Moreover, covert communication or information hiding is still needed even if the transmitted information has been encrypted in army or intelligence agencies. A great deal of data also brings a huge difficulty to information hiding for color image. Many encryption algorithms currently do not consider the compression problem of image data[1][2]. The essence of these encryption algorithms is changing the pixel positions or values of image, and the correlation between pixels is damaged. Therefore, image is hard to compress again. Correlation between some pixels is retained using simple block scrambling or a method of changing transform domain coefficient to continue to compress encrypted image in the literature [3][4]. However, these several ways cannot withstand plaintext attacks. Many studies on image hiding technology are watermark technology research based on the purpose of copyright protection [5][6]. Watermark images are generally binary images or gray images, so there are few color images. These information hiding methods are applicable for watermark data with smaller data amount. The transparency and robustness of information hiding can only be sacrificed when the amount of data needing secure communication increases. Therefore, hidden information security will not be guaranteed.

The secure communication scheme proposed in this paper uses a way of combining encryption and hiding. Secret image is encrypted, while image data is compressed. Thus, the amount of data to be hidden will be reduced for the same size of image, and the transparency of information hiding is guaranteed.

II. ENCRYPTION PROCESS

Encryption process consists of two parts: (1) Secret image encryption process: index-value acquisition process and data compression process. (2) Secret image hiding process: the process of embedding a secret image into a public transmission image. Encryption process is shown in Fig.1.

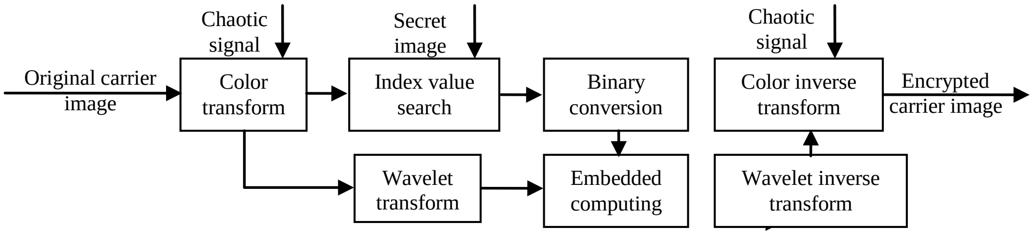

Figure 1. Encryption process

A. Preprocessing of carrier image

A palette was built by preprocessing carrier image before the index value of secret image was obtained. Pretreatment process is the process of scrambling and confusing carrier image by using chaotic signal. Purposes were as follows:

- The anti-attack capability of encryption system was improved.
- The number of colors in the image carrier was increased.
- The color distribution law of image carrier was changed so that the color distribution had the uniform, random characteristics.

Assume that a carrier image was a color image ***A*** with MA×NA size which can be expressed as : $A = \{a(i, j, k), 1 \le i \le MA, 1 \le j \le NA, 1 \le k \le 3\}$. Moreover, its three color components were ***AR***, ***AG*** and ***AB*** which can be expressed as: $AR = \{ar(i, j), 1 \le i \le MA, 1 \le j \le NA\}$, $AG = \{ag(i, j), 1 \le i \le MA, 1 \le j \le NA\}$, $AB = \{ab(i, j), 1 \le i \le MA, 1 \le j \le NA\}$ .where ar(i, j)=a(i, j, 1), ag(i, j)=a(i, j, 2) and ab(i, j)=a (i, j, 3). Hence, chaotic system would generate two chaotic sequences with lengths of MA and NA, respectively which were used to transform the location of carrier image pixel. Then, a chaotic sequence with a length of MA×NA×3 was generated which was used to modify carrier-image pixel values.

1) Generation of chaotic sequence: Chaotic mapping is widely used in encryption system [7][8]. The initial conditions of chaotic sequence have many features such as extreme sensitivity, aperiodicity, pseudo-randomness and rapid regeneration. Therefore, the mapping used these features to perform the scrambling and confusion on secret signal so as to achieve an encryption purpose. Chaotic signal in this paper, unlike it, acts on carrier image. Moreover, the main purpose was to increase the number of colors in a carrier image so that carrier image colors were evenly distributed.

Chebyshev mapping was used to generate chaotic sequence in this study [9]. The expression of K-order Chebyshev mapping is shown in (1) below:

$$x_{n+1} = \cos(k \cos^{-1} x_n) \qquad (1)$$

Equation (1) is a one-dimensional chaotic mapping that is a full mapping of interval [-1,1] to interval [-1,1]. Its iterative equation is simple and easy to implement.

If the gray level of carrier image is N, then the chaotic sequence is mapped to [0, N-1] range. Its method is shown in (2) below:

$$X(i) = \left| \lfloor x(i) \rfloor \times M \right| \bmod N \qquad (2)$$

2) Carrier image scrambling: The scrambling of carrier image by chaotic sequence used the method of first row scrambling and then column scrambling, and these steps are as follows:

- Sequences H and L with lengths of MA and NA were produced by Formula (1), respectively.
- The sequence H was reordered from small to large to form a new sequence H'.
- Each row of the carrier image was rearranged according to the migration laws of each element position from sequence H to sequence H'. That is, if: H'(m)=H(n), then the n-th row of pixel in the carrier image would be moved to the m-th row.
- The sequence L was reordered from small to large to form a new sequence L'.
- Each column of carrier image was rearranged according to the migration laws of each element position from sequence L to sequence L'. That is, if: L'(m)=L(n), then the n-th column of pixels in the carrier image will be moved to the m-th column.

3) Color conversion of carrier image: The pixel values of carrier image were changed through chaotic sequence using the following method:

Chebyshev sequences were generated by (1). Then, the data with relatively large absolute value were removed, leaving MA×NA×3 state values. Three matrixes ***RR***, ***RG*** and ***RB*** were generated through the mappings of state values according to (2), which can be expressed as: $RR = \{rr(i, j), 1 \le i \le MA, 1 \le j \le NA\}$, $RG = \{rg(i, j), 1 \le i \le MA, 1 \le j \le NA\}$ and $RB = \{rb(i, j), 1 \le i \le MA, 1 \le j \le NA\}$

The color conversion of carrier image was performed according to (3).

$$\begin{cases} car(i, j) = ar(i, j) \oplus rr(i, j) \\ cag(i, j) = ag(i, j) \oplus rg(i, j) \\ cab(i, j) = ab(i, j) \oplus rb(i, j) \end{cases} \qquad (3)$$

The carrier image was recorded as ***CA*** after color conversion: $CA = \{ca(i, j, k), 1 \le i \le MA, 1 \le j \le NA, 1 \le k \le 3\}$, and its three color components ***CAR***, ***CAG*** and ***CAB*** can be expressed as: $CAR = \{car(i, j), 1 \le i \le MA, 1 \le j \le NA\}$, $CAG = \{cag(i, j), 1 \le i \le MA, 1 \le j \le NA\}$ and $CAB = \{cab(i, j), 1 \le i \le MA, 1 \le j \le NA\}$.

B. Index value acquisition of secret image

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations. Assume that a secret image was a color image ***W*** with a MW×NW size which can be expressed as: $W=\{w(i,j,k),1\le i\le MW,1\le j\le NW,1\le k\le 3\}$. Moreover, its three color components were ***WR***, ***WG*** and ***WB*** which can be expressed as: $WR=\{wr(i,j),1\le i\le MW,1\le j\le NW\}$, $WG=\{wg(i,j),1\le i\le MW,1\le j\le NW\}$ and $WB=\{wb(i,j),1\le i\le MW,1\le j\le NW\}$, where wr(i, j)=w (i, j, 1), wg(i, j)=w (i, j, 2) and wb(i, j)=w (i, j, 3).

The index values of secret image were determined by calculating Euclidean distance between the pixel value of each point in secret image and carrier image. Specific steps were as follows:

The first step was to determine the search extent of carrier image. The carrier image was divided into S regions, and each region has a size of MS×NS. Moreover, the values of MS and NS cannot be too small or too big. Too small may make image distortion large, but too large may increase the amount of data to be hidden and the difficulty of information hiding. The 16≤MS≤256 and 16≤NS≤256 were generally taken. Index values are obtained by search in the any area of carrier image above to reconstruct secret images. Experiments show that these images almost have no difference because the carrier image colors are evenly distributed.

There were Euclidean distances between the pixel values of some point with a subscript (i, j) in secret image and each point in carrier-image search area. The second step was to calculate them according to (4).

$$ED(m,n)=\sqrt{\sum_{k=1}^{3}(w(i,j,k)-a(m,n,k))^2} \qquad (4)$$

There were 1≤m≤MS and 1≤n≤NS in (4).

The third step was to find (m, n) value with the minimum Euclidean distance, which is the index value of pixel point with a subscript (i, j) in secret image.

The fourth step was to code index values to a binary data stream which was recorded as ***B***.

C. Embedding of secret image

Secret-image embedding steps were as follows:

Step 1, carrier image ***A*** was divided into several areas after chaotic transformation, and the size of each area was I×J. The lifting wavelet transform of each R, G and B primary color component was performed in each region to extract low frequency component coefficients to be processed.

Step 2, threshold was adaptively set according to the length of data stream ***B***, and a coefficient with greater energy was extracted. Methods were as follows: the wavelet coefficients of each component were sorted in descending order, and the sorted wavelet coefficients were: $Ar=\{ar(k),1\le k\le I\times J/4\}$, $Ag=\{ag(k),1\le k\le I\times J/4\}$ and $Ab=\{ab(k),1\le k\le I\times J/4\}$, respectively. If the data length of stream ***B*** (i.e., binary digital bit is included in B) is LB, then the domain values of three components are Tr=ar(LB), Tg=ag(LB) and Tb=ab(LB), respectively.

Step 3, the spread spectrum processing of index value was first performed after coding, and then the selected wavelet coefficients were modified. Suppose that *AWr, AWg* and *AWb* were the selected wavelet coefficients, and *b* was binary digital. The embedded data of coefficients were modified according to (5):

$$\begin{cases} Awr=AWr(1+\alpha r(2\times b-1)) \\ Awg=AWg(1+\alpha g(2\times b-1)) \\ Awb=AWb(1+\alpha b(2\times b-1)) \end{cases} \qquad (5)$$

The ar, ag and ab were embedding strength, and the strength size relates to the robustness and concealment of watermark. If visual sensitivity was considered, then embedding intensity in the green component may be larger, and embedding intensity in blue component was relatively small. It is found that the embedding intensity of blue component cannot be too small to consider robustness in the experiment. The actual values meet ar<ag<ab<0.09.

Step 4, carrier image hiding index values was obtained through chaotic transformation after wavelet inverse transform.

III. Decryption process

Decryption process included two processes: extraction of embedded index value and encrypted image reconstruction. Decryption process is shown in Fig.2.

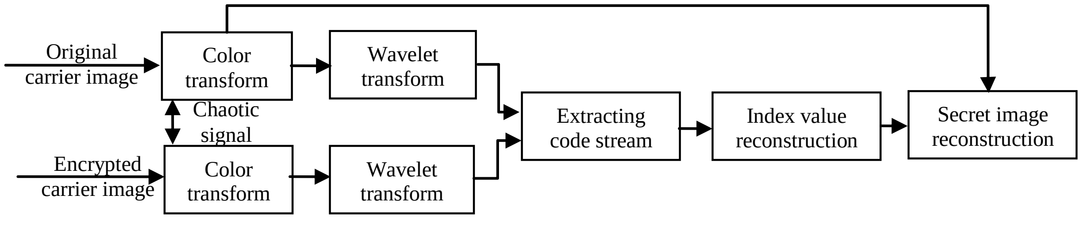

Figure 2. Decryption process

The chaos transform and lifting wavelet transform were done to the original carrier image and encrypted carrier image respectively in the first step. Moreover, wavelet coefficients were selected in accordance with the same method in chapter 2 section C.

Compressed bit streams were extracted by inverse operation using same embedding coefficients in the third step of chapter 2 section C to reconstruct index value in the second step.

The chaotic transformation of original carrier image was performed according to the same key in chapter 2 section A in the third step. The corresponding pixel points were found in the selected search area. Secret image is reconstructed on the basis of the extracted index values.

IV. Simulation experiment

Simulation experiment was done in Matlab7.0 simulation environment. Many carrier images and secret images were arbitrarily selected in experiments, and several simulations were conducted. Results show that this algorithm is feasible. The following experiments used 2048×2048 24bit true color image "Orchid Series Red.jpg" as vector image. The 90×90 24bit true color image " Suzhou maps.jpg" was selected as the secret image. Simulation experiment included the analyses and comparisons on following four aspects of content:

- Carrier image before and after chaotic transformation;
- The compression rates of compressed images and the qualities of reconstructed images;
- Image hiding transparency before and after compression;
- The robustness of encryption algorithms.

A. Chaotic transformation of carrier image

The histograms of original carrier image and its red component distribution are shown in Fig.3 (a) and (b) respectively:

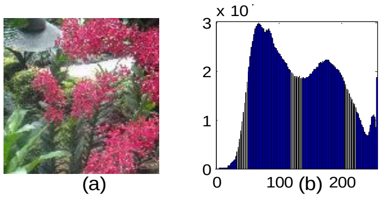

Figure 3. Original carrier image and red component distribution

A row scrambling sequence with a 2048 length and a column scrambling sequence were produced, respectively by taking k=5 and x0=0.6 in (1). The histograms of carrier image and its red components are shown in Fig.4 (a) and (b) after scrambling in accordance with each step in chapter 2 section A part 2.

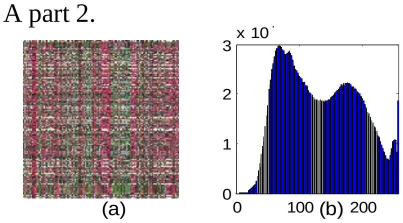

Figure 4. Scrambling carrier image and red component distribution

The comparison of Fig.3 and Fig.4 shows that scrambling changes each pixel position in the image, but cannot change the statistical distribution law of pixels.

A chaotic sequence with 2048×2048 state values were produced by taking k=5 and x0=0.9 in (1). The histograms of carrier image and red component distribution are shown in Fig.5 (a) and (b) after its color transformation according to each step in chapter 2 section A part 3.

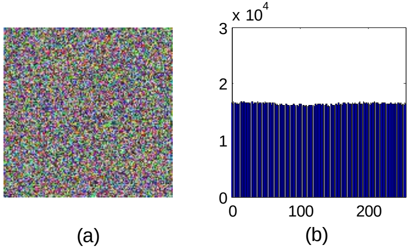

Figure 5. Carrier image and red component distribution after color transformation

The comparison of Fig.3 and Fig.5 shows that the statistical law of carrier-image color distribution is significantly changed. Thus, the color distribution is very uniform.

B. Image Compression and Reconstruction

Index values were obtained in different carrier images, and the secret image was reconstructed by the index values. Similarity between original image and the secret image reconstructed by index values was calculated according to the reference [10]. The compression ratio of image data was calculated by (6).

Compression ratio formula is:

$$CR = \frac{\text{image data after compression}}{\text{image data before compression}} \times 100\% \qquad (6)$$

When the search area of index value was changed, compressed secret-image data amount, compression rate and similarity between reconstructed image and original image were calculated. Results are shown in Table 1.

TABLE 1 COMPRESSION RATIO AND IMAGE QUALITY COMPARISON

Search area	**Compressed data amount/bit**	**Compression rate**	**Similarity**
Original image 2048×2048	90×90×2×11	0.91667	0.99738
Transformed image 2048×2048	90×90×2×11	0.91667	0.99993
Transformed image 1024×1024	90×90×2×10	0.83333	0.99983
Transformed image 512×512	90×90×2×9	0.75000	0.99955
Transformed image 256×256	90×90×2×8	0.66667	0.99894
Transformed image 128×128	90×90×2×7	0.58333	0.99708
Transformed image 64×64	90×90×2×6	0.50000	0.99370
Original image 64×64	90×90×2×6	0.50000	0.11936

Similarity between reconstructed image and original image in Table 1 shows that reconstructed image quality is relatively poor if index values are searched in original image. The reconstructed secret image of higher quality can be obtained if index values are searched in a small area of carrier image after color transformation. Thus, the secret image data can obtain a higher compression ratio. Similarity between reconstructed image and original secret image can still exceed 99% when image data is compressed into a half, thus maintaining a good reconstruction quality.

C. Analysis of information hiding transparency

The secret image and carrier image after information embedding is shown in Fig. 6 (a) and (b).

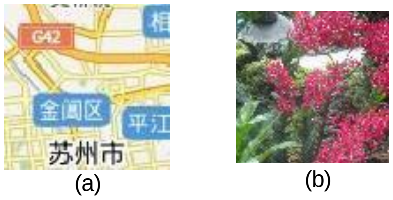

Figure 6. Secret image and carrier image

The original secret image and secret image after compression encryption were respectively embedded in the carrier image, the visual difference cannot be found.

The peak signal to noise ratio was calculated by (7) before and after data were embedded in the carrier image. When the original secret image was embedded in the carrier image, the peak signal to noise ratio is 36.32881, and when the compressed secret image was embedded in the carrier image, the peak signal to noise ratio is 38.31003. The greater the signal to noise ratio is, the better the image quality is maintained and the better the transparency of information hiding is. Therefore, the use of compression and encryption algorithms can improve the transparency of information hiding.

$$PSNR = 10\log_{10}\left(\frac{XYZ \max\limits_{x,y,z} A^2{}_{x,y,z}}{\sum\limits_{x,y,z}(A_{x,y,z} - Aw_{x,y,z})^2}\right) \qquad (7)$$

where, $A_{x,y,z}$ represents the pixel point in original image, $Aw_{x,y,z}$ represents the pixel point in carrier image with embedded secret data, x and y are row and column, respectively, Z value is 1, 2 or 3.

D. Robustness Analysis

The compression, adding noise, cutting, filtering and other operations on carrier image were conducted in simulation experiments, and reconstructed image qualities were compared. Moreover, the similarity was calculated between reconstructed secret image and image without an attack. Encryption algorithm robustness was analyzed.

Image compression simulation used the JPEG compression. The carrier image before and after compression are 644kB and 412kB with the quality factor of 60, respectively. Carrier image after compression and reconstructed secret image are shown Figures 7 (a) (b), respectively, and the similarity is 0.87341 between extracted secret image and original secret image.

Salt-pepper noise with an intensity of 0.02 was added into the carrier image in adding noise experiment. Carrier image with noise and reconstructed secret image are shown Fig.7 (c) and (d), respectively. Similarity is 0.93516 between extracted secret image and original secret image.

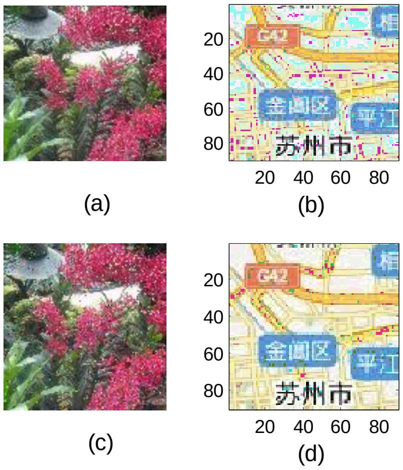

Figure 7. Compression and noise test

Carrier image after cutting and reconstructed secret image are shown in Fig.8 (a) (b), respectively, and the similarity of reconstructed secret image and original image is 0.73482. Fig.8(c) shows carrier image after the median filter of window that is 3. Fig.8 (d) shows reconstructed secret image after median filter, and similarity is 0.86824 between reconstructed secret image and original image.

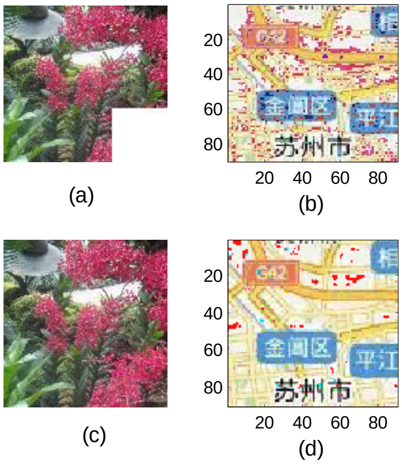

Figure 8. Cutting and filter test

V. CONCLUSIONS

An encryption compression algorithm was proposed. As can be seen from the simulation experiments, a larger effect of data compression is obtained with a very little loss of quality by this algorithm. Thus, the data amount of information hiding is reduced, and the transparency of information hiding is improved. The proposed encryption compression method is used in the time domain of carrier image, so the anti-attack ability is weaker. However, the encryption compression method may be used on a white image without relying on carrier image. Therefore, encryption and compression on secret image can be independently conducted, completely independent of the carrier image. Then, the ability to resist attacks of secure communication entirely depends on embedding algorithm. The secure communication scheme of color image has implemented the following innovation:

- Traditional encryption thinking is changed, and encryption is achieved no longer by changing image pixel position or pixel value.
- Encryption and compression can be performed at the same time, and a larger amount of data compression is obtained with a minimal loss of quality.
- The introduction of index technology into image encryption and compression makes hidden data amount reduced.
- The combination of encryption and hiding makes communication security improved.

REFERENCES

[1] A. Akhavan, A. Samsudin, and A. Akhshani, "A symmetric image encryption scheme based on combination of nonlinear chaotic maps," Journal of the Franklin Institute, 2011,348(8), pp.1797-1813.

[2] G. Zhang, Q. Liu, "A novel image encryption method based on total shuffling scheme," Optics Communications, 2011, 284(12), pp. 2775-2780.

[3] S. G. Lian, J. S. Sun, and Z. Q. Wang, "A novel image encryption scheme based on JPEG encoding," Proc. of the 8th International Conference on Information Visualisation, 2004,pp. 217-220.

[4] X. Ge, F. L. Liu, B. Lu, "An image encryption algorithm based on spatiotemporal chaos in DCT domain," Proc. of the 2nd International Conference on Information Management and Engineering, 2010, pp. 267-270.

[5] H. Peng, J. Wang, W. X. Wang, "Image watermarking method in multiwavelet domain based on support vector machines," Journal of Systems and Software, 2010,83 (8), pp. 1470-1477.

[6] Z. H. Li , H. Z. Wu, "Geometrically robust image watermark based on DWT and steerable pyramid," Journal of Image and Graphics, 2010,15(2), pp. 211-219.

[7] Z. Tao, H. M. Zhao, J. Wu, "Research on digital audio watermarking algorithm based on lifting wavelet transform and chaotic keys," ACTA ACUSTICA, 2011,36(6), pp. 665-674.

[8] G. Xu, Y. D. Zhang, X. X. Zhang, " Digital image encryption algorithm based on an alternating iterative chaotic System," Journal of University of Science and Technology Beijing, 2012, 34(4), pp. 464-470.

[9] J. M. Gu, W. X. Hong, T. Liang, " Improvable Chebyshev Chaotic Sequence and Performance Analysis," Journal of Military Communications Technology, 2006, 27(1), pp. 43-46.

[10] J. Y. Peng, S. R. Gong, "Encryption and Compression Scheme of Color Image Based on a Hyperchaotic System," International Journal of Online Engineering, 2013, 9(s6), pp. 73-77.