Computer Engineering and Intelligent Systems www.iiste.org
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.5, No.9, 2014

Digital Rights Management: Improving Online Digital Images Copy Rights Management through an Enhanced Least Significant Bit Steganographic Algorithm

Gabriel Macharia Kamau[1]* Dr. Cheruiyot W. K[2]

1. School of Computer Science and Information Technology, Dedan Kimathi University of Technology, PO box 657-10100, Nyeri, Kenya
2. Institute of Computer Science and Information Technology, Jomo Kenyatta University of Agriculture and Technology, PO box 62000-00200, Nairobi, Kenya

* E-mail of the corresponding author: ngorosh2003@yahoo.com

Abstract

Digital media no doubt presents numerous advantages compared to the traditional analog media. Of the most importance is the fact that digital content (images, graphics, audio and video) can be easily copied, transmitted, retrieved and distributed over private and open access networks. The global availability of the internet- certainly the most impactful information exchange tool today- plus the numerous file sharing tools freely available have made the distribution of copyrighted digital media files simple and straightforward.

Duplication of exact copies of original images, for example can be easily done and circulated without authentication. As much as this is an advantage in trying to enhance sharing of information, it certainly creates problems of ownership and authenticity and digital rights protection. There already exists copyright laws that provide for protection of all online content but the task of continuously guarding the web and correctly identifying those that infringe against these laws is increasingly becoming enormous. There is therefore need to continuously invest in development of new technologies and algorithms that will make it more and more difficult to illegally copy or use someone else content.

To improve security of copyrighted online digital images, this paper proposes the use of an enhanced LSB steganographic algorithm that employs a selective and randomized approach in picking specific number of target image bits to swap with the owners signature authentication bits using a pseudo random number generator (PRNG). The carefully selected password seed is used to determine the set of selected numbers used for targeting specific image bits for the signature hiding.

An experimental design is setup to determine the effectiveness of the method by comparing and analyzing the stego images' statistical characteristics and the ability of steganalysis methods to detect the hidden signature.

The experimental results indicate improved levels of imperceptibility and hence improved security against illegal copying.

Keywords: Digital Media, Steganography, Copyright, Steganalysis, Stego image, imperceptibility

1. Introduction

Lack of proper and continuously improved tools and algorithms to ensure digital content copy rights protection contributes significantly to hindered growth of multimedia networked services as publishers and authors of multimedia data and information continue to hesitate in endorsing distribution of their material in open access networked environments. (Mei et al .2009).

Improved algorithms of steganography as a means of covert communication can be used to imperceptibly embed digital signatures in digital data before distribution to enhance authenticity. According to Mohammad and Abdallah (2008), Steganography "is the art and science of writing hidden messages inside innocent looking containers, specifically digital files, in such a way that no one apart from the sender and intended recipient realizes the existence of the hidden message". This secret message can constitute digital signatures for copy righted material to enhance authenticity and detect unauthorized duplication of digital data.

One of the most popular and commonly used steganographic algorithms in digital images is the Least Significant Bit (LSB) insertion method. It is a simple algorithm that swaps the least significant bit in some bytes of the cover medium with a sequence of bytes containing the secret data to be hid. However, though the LSB algorithm hides data in the cover medium (image) in a way that is imperceptible to the Human Visual System (HVS), its imperceptibility to statistical steganalysis is relatively low. This is mainly because the significant bits of the secret message are hidden in the cover medium in a linear and deterministic pattern. Retrieval of secret data using steganalysis software tools therefore becomes relatively easy once the algorithm used is known. The use of an enhanced LSB method which utilizes varied and random bits in a true color image to embed the confidential message is proposed in this paper.

2. Related Work

2.1 The Optimal LSB Insertion Method

This insertion method improves the stego-image quality by finding an optimal pixel after performing an adjustment process. Three candidates are picked out for the pixel's value and compared to see which one has the closest value to the original pixel value with the secret data embedded in. The best candidate is then called the optimal pixel and used to conceal the secret data (Chan and Cheng, 2004). This however makes the hiding capacity of the carrier image very low.

2.2 The Pixel Value Differencing (PVD) Method

The pixel-value differencing (PVD) method is proposed by (Wu and Tsai, 2003). In this approach, the payload of each individual pixel is different, and the resultant stego-image quality is extremely fine with perfect modification and invisibility. The resultant stego-images quality that the method produces is better in terms of human visual perception. However steganalysis is easy as the hidden message is not well spread across the entire image.

2.3 Blind Hide algorithm

According to (Bailey, K. & Curran, K. 2006), this algorithm blindly hides the secret data in the image starting at the top left corner of the image and working its way across the image (then down - in scan lines) pixel by pixel changing the least significant bits of the pixel colors to match the message. To extract the hidden information, the least significant bits starting at the top left are read off. This embedding procedure is not very secure as it's really easy to read off the least significant bits starting from the top left corner of the image sequentially.

2.4 Algorithm Pixel Swap

This method is proposed by Lee et al. (2010). It works as follows

- Randomly select 2 pixels x1 and x2 from the cover image using a pseudo–random sequence.
- If the two pixels lie within a specified distance α (α=2 or 3 generally), they are suitable for embedding, otherwise generate another set of pixels.
- Take the specific message bit to hide. If the message bit is zero, check if x1 > x2 otherwise swap x1 and x2 and hide the bit in the LSB of the pixel. Do the reverse operation if the message bit is one.
- For extracting the hidden message, select the pixels using the same pseudo-random sequence. Check if the 2 pixels are within the pre-specified range α. If x1>x2, the message bit is zero (one) otherwise the message bit is one (zero).

This method does not add visible distortions to the cover image since only one bit is changed per pixel but its hiding capacity is highly limited. An implementation of this is Hermatic stego version 9.3

3. The Proposed Method

The use of an enhanced LSB method which utilizes varied and random bits in a true color image to embed the confidential message is proposed in this paper. The Linear Congruential Generator (LCG) method proposed by D.H. Lehmer is used to generate the pseudo random numbers used to match the specific bits in the cover image where the secret author's signature bits are hid. LCG method is one of the most successful random number generators. It is also fast and saves on computer memory.

The formula is explained below.

Xn+1 =(aXn + c) mod m (1)

Where:

X0 is the starting value , the seed ; 0 <=X0 < m

a is the multiplier; a ≥ 0

c is the increment; c ≥ 0

m is the modulus; m > X0, m > a, m > c

The desired sequence of random numbers < Xn > is then obtained by setting

Xn+1 =(aXn + c) mod m, n ≥ 0

Xn is chosen to be in [0, m-1], n ≥0

Given that the previous random number was Xi, the next random number Xi+1 can be generated as follows.

X i+1 = f (Xi, X i-1,…., X i-n+1)(mod m) = (aix i+ a2 x i-1 +…+ an x i-n+1 + c)(mod m)

A stego key (k) is used during extraction which in this case is the message digest of the user supplied password.

According to Hull & Dobell (1972), a linear congruential sequence defined by m,a,c and X0 has full period if and only if the following three conditions hold:

- The only positive integer that exactly divides m and c is 1
- If q is a prime number that divides m, then q divides a -1
- If 4 divides m, then 4 divides a -1

Additionally, the value of m should be rather large since the period cannot have more than m elements. The value of m should also necessitate a fast computation of (aXn+c) i.e speed the generation of random numbers. Observing all these requirements, the parameters for the LCG picked as follows:

Modulus (m)

The 48-bt computer word length was picked as the value of m. This in essence provides the size of m to be 248 which is equivalent to 281,474,976,710,656. For the sake of this experiment and bearing in mind that the digitals images used are a few kilobytes in size, this period is sufficient enough to set up the experiment.

To ensure faster generation, m is recommended to be a power of 2 or close to a power of 2 and hence the choice of the word length. Using the AND operation also enhance speed instead of the normal division operation which is considered slower.

The seed (X0)

The first value of the seed (X0) is supplied by the message digest of the user supplied password. This is done using a special form of encryption that uses a one-way algorithm which when provided with a variable length unique input (message) will always provide a unique fixed length output called hash, or message digest.

Multiplier (a) and Increment (c)

To ensure full period and in following with requirements identified above, the values of the multiplier and the increment are picked as follows.

a (Multiplier) = 25214903917

c (Increment) = 11

The values are used to initialize the random number generator used for the experiment.

The numbers generated by this PRNG determines the specific bits in the pixel bytes of the cover image where data bits of the secret data file are to be embedded. For example considering storing the 200, which binary representation is 11001000 in a grid of 3 pixels of a 24-bit image, utilizing a single LSB of each color channel the enhanced LSB algorithm will store the significant bits of the message randomly into the cover image bits as shown in Tables 1 and 2.

Table 1. Original Image Bits

0	0	1	0	1	1	0	1	0	0	0	1	1	1	0	0	1	1	0	1	1	1	0	0
1	0	1	0	0	1	1	0	1	1	0	0	0	1	0	0	0	0	0	0	1	1	0	0
1	1	0	1	0	0	1	0	1	0	1	0	1	1	0	1	0	1	1	0	0	0	1	1

Table 2. Modified Image Bits

0	0	1	0	1	1	1	1	0	1	0	1	1	1	0	0	1	1	0	1	1	1	0	0
0	0	1	0	0	1	1	0	1	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0
1	1	0	0	0	0	1	0	1	0	1	0	1	1	0	1	0	1	1	0	0	0	1	0

4. Research Method

The experimental research method is used in measuring the effect of using selected varied and random pixels during the embedding process on imperceptibility. This method represents the standard practice applied in manipulating independent variables in order to analyze the generated data to test the research hypotheses. A notable advantage of experimental research is the fact that it enables other researchers to easily replicate the experiment and be able to validate the results. It is therefore considered an accurate method of research (Shuttleworth, 2008), as the researcher can effectively establish a causal relationship between variables by manipulating independent variable(s) to assess the effect upon dependent variable(s).

An experiment was carried out to test the relationship between the specific embedding process (i.e. proposed method) and the outcome (i.e. imperceptibility level). Essentially the output of traditional least significant bit steganography method was used to evaluate the performance and effectiveness of the proposed method's output by comparing the stego images generated by the proposed method with those generated by the traditional least significant bit steganography method. This is commonly referred to as comparative experiment (Hinkelmann and Kempthorne, 2008).

4. Experimental Design and Testing

An analysis to examine the statistical properties of the stego images produced by the proposed method and the traditional LSB method was carried out. Statistical attacks are more powerful than visual attacks as they are able to reveal the tiniest modifications in the statistical properties of an image (Artz, 2001).

The following image quality metrics were employed for this purpose.

4.1 Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE)

Both of these metrics are the most common and widely used full reference metrics for objective image quality evaluation. In particular, PSNR is used in many image processing applications and considered as a reference model to evaluate the efficiency of other objective image quality evaluation methods (Wang et al., 2002b). PSNR as a metric computes the peak signal-to-noise ratio, in decibels, between two images. It is used in steganography to measure the peak signal-to-noise ratio in the original image and the stego image after embedding the hidden data. In the literature, PSNR has shown the best advantage almost over all other objective image quality metrics under different image distortion environments and strict testing conditions (Wang et al., 2002a).

On the other hand, MSE measures the statistical difference in the pixel values between the original and the reconstructed image (Stoica et al., 2003; Wang et al., 2003). The mean square error represents the cumulative squared error between the original image and the stego-image. PSNR and MSE are defined in equation 1 and equation 2 below (Stoica et al., 2003; Wang et al., 2003).

$$MSE = \left(\frac{1}{MN}\right) \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X_{ij} - \overline{X_{ij}} \right)^2 \qquad (2)$$

$$PSNR = 10.\log_{10} \frac{I^2}{MSE}\, db \qquad (3)$$

Where:

Xij is the ith row and the jth column pixel in the original (cover) image,

Xij is the ith row and the jth column pixel in the reconstructed (stego) image,

M and N are the height and the width of the image ….in equation 1.

I is the dynamic range of pixel values, or the maximum value that a pixel can take, for 8-bit images: I=25 ……in equation 2.

A lower MSE value means a better image quality ie lesser distortion in the cover image while the higher the PSNR value the better the quality of the image. (Mei et al .2009).

In order to evaluate the performance of the proposed method an experimental design was set up. Stego images from both the traditional LSB method and the proposed method were compared using the testing metrics discussed above. All the experiments were implemented and run on a PC Pentium IV Duo core, 2.1 GHz with 2GB of RAM under the Windows 7 Home Edition operating system. The following constants were ensured.

- Same images were used on both the methods
- Same information was embedded in each image ie equal payload
- Same evaluation metrics were used for each image
- Five digital pass port size face images were used as test data files (cover images). Table 3 shows the list of these digital images.

Table 3. Test Data Images

FILE NAME	DIMENSIONS	FILE SIZE
Banana.jpg	685 x 514 Pixels	157 Kilo Bytes
Dancers.jpg	685 x 457 Pixels	224 Kilo Bytes
Graduation.jpg	685 x 457 Pixels	161 Kilo Bytes
Office.jpg	685 x 457 Pixels	163 Kilo Bytes
zhbackground.bmp	685 x 610 Pixels	1.19 MB

The specific data hiding steganogrtaphic method used was taken to be the independent variable (in this case the traditional LSB method and the proposed enhanced LSB method). In order to evaluate the efficiency of the proposed steganography method, the evaluation dependent variables which measure the image distortion levels were considered. Accordingly, for each steganography method (the traditional LSB method and the proposed enhanced LSB method) and for each cover image the value of each dependent variable was measured. The values of the dependent variables for both embedding methods were then compared.

Table 4 below shows a comparison of the PSNR values of the five stego images for both the traditional LSB and the Enhanced LSB methods

Table 4. The PSNR of stego images generated by the two data hiding methods

Image	**Traditional LSB (db)**	**Enhanced LSB (db)**	**Difference (db)**
Banana.jpg	63.4	66.5	3.1
Dancers.jpg	62.8	65.4	2.6
Graduation.jpg	56.4	57.8	1.4
Office.jpg	62.9	65.5	2.6
zhbackground.bmp	57.6	59.4	1.8

Table 5 below is a summary of the MSE of the seven stego images after hiding data using the least significant bit method and the enhanced method as generated by the Digital Invisible Ink Toolkit. From all the five test data images used, each recorded a lower mean square error when the enhanced LSB was used as compared to the traditional LSB method. A lower MSE value means a better image quality ie lesser distortion in the cover image (Mei Jiansheng et al .2009). This means that stego images generated by the enhanced LSB method have lesser distortions compared to those generated by the traditional LSB method and hence improved imperceptibility.

Table 5. The MSE of stego images generated by the two data hiding methods

Image	**Traditional LSB (db)**	**Enhanced LSB (db)**	**Difference (db)**
Banana.jpg	0.268	0.146	0.122
Dancers.jpg	0.304	0.165	0.139
Graduation.jpg	1.34	0.961	0.379
Office.jpg	0.302	0.164	0.138
zhbackground.bmp	1.003	0.664	0.339

5. Experimental Results

5.1 Peak Signal to Noise Ratio (PSNR)

Figure 1 below shows the comparison of the PSNR of five stego images for both the traditional LSB method and the enhanced LSB method.

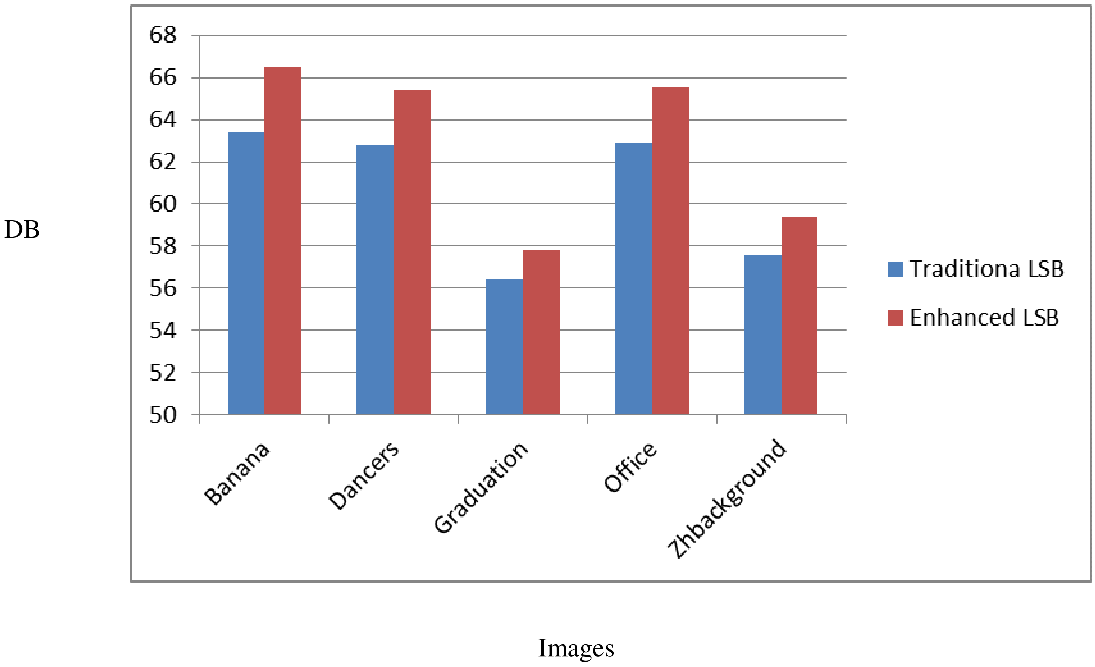

Figure 1: The PSNR (DB) of stego images hiding in (Traditional LSB) vs hiding in (Enhanced LSB)

Every image tested registered a higher PSNR for enhanced LSB method as compared to the Traditional LSB method showing that the enhanced LSB embedding method distorts the image less improving on imperceptibility of the hidden data since a higher Peak Signal to Noise Ratio (PSNR) indicates less distortion (Mei Jiansheng et al .2009).

5.2 *Mean Square Error (MSE)*

Figure 2 shows a summary of the comparison of the MSE of five stego images for both the traditional LSB method and the enhanced LSB method.

For each stego image, a lower MSE was recorded with the enhanced LSB method as compared to the traditional LSB method. A lower MSE value means a better image quality ie lesser distortion in the cover image (Mei Jiansheng et al .2009). This means that stego images generated by the enhanced LSB method have lesser distortions compared to those generated by the traditional LSB method and hence improved imperceptibility.

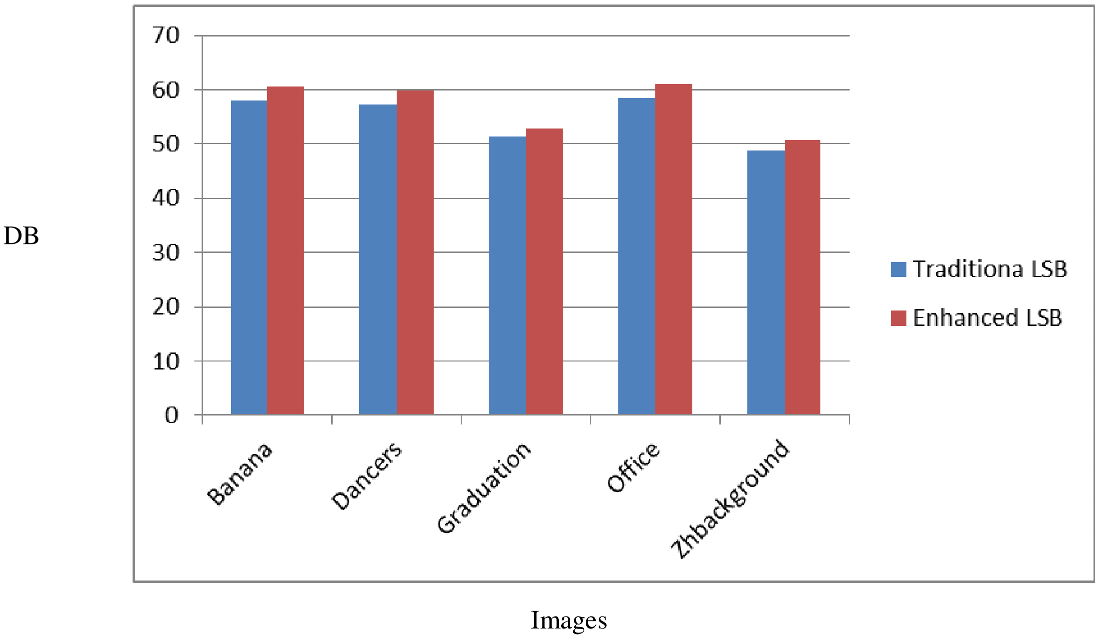

Figure 2: The MSE of stego images Hiding in (Traditional LSB) vs Hiding in (Enhanced LSB)

6. Conclusion and Future Work

In this paper, an improved digital image copyright protection algorithm based on an improved LSB steganographic method has been presented. The purpose is to embed the signature of the owner of a digital image in his file in order to aid in authentication of original copyrighted files. The signature is embedded in a more imperceptible manner as compared to the way a conventional LSB method would do. There is a demonstration of increased imperceptibility to statistical steganalysis attacks on the cover image as proved through the perceptibility metrics used thereby enhancing security of the authors work.

References

Artz D. (2001) “Digital steganography: hiding data within data”, Internet Computing, IEEE, vol. 5, Issue: 3, pp. 75-80

Bailey, K. and Curran, K. (2006) An Evaluation of Image Based Steganography Methods Using Visual Inspection and Automated Detection Techniques. Multimedia Tools and Applications, 31, 55-88.

Chan, and Cheng, L.M. (2004). Hiding data in images by simple LSB substitution. Computer Journal of Pattern Recognition Letters, vol. 37, no. 3, pp. 469-474

Chang, K. I., Bowyer, K. W., Flynn, P. J.(2005) Evaluation of Multimodal 2D+3D Face Biometrics. IEEE Transactions on Pattern Analysis and Machine Intelligence, 27(4):619–624

Fridrich, J., Goljan, M. and Hogea, D. (2002) Attacking the OutGuess. The ACM Workshop on Multimedia and Security.

Jain, A.K., and Jianjiang, F.(2011). Latent Fingerprint Matching. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.33, no.1, pp.88-100.

Lee, Y.K., Bell, G., Huang, S.Y., Wang, R.Z. , Shyu, S.J. (2010). An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding. Advances in Image and Video Technology. Berlin / Heidelberg: Springer, 349-360.

Hinkelmann, K. & Kempthorne, O. (2008) Design and Analysis of Experiments: Introduction to Experimental

Design, John Wiley & Sons, Inc., Hoboken,New Jersey.

Mei, J., Sukang, l., and Xiaomei, T.(2009) "A Digital Watermarking Algorithm Based on DCT and DWT", in Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, pp. 104-107.

Mohammad, F. and Abdallah, M. (2008). "A Steganographic Data Security Algorithm with Reduced Steganalysis Threat," Birzeit University, Birzeit.

Pfitzmann (1996). 'Information Hiding Terminology', In:Information Hiding: First International Workshop (R Anderson, ed), Lecture Notes in Computer Science 1174, pp 347-350, Berlin: Springer-Verlag.

Wu, D.C. and Tsai, W.H. (2003). A steganographic method for images by pixel value differencing. Pattern Recognition Letters. Vol. 24 (9-10), 1613-1626.

Shuttleworth, M. (2008) Experiment Resources. Accessed: September 25, 2011. URL:

http://www.experiment-resources.com. Accessed on 10th June 2014.

Stoica, A., Vertan, C., Fernandez-Maloigne, C. (2003) Objective and subjective color image quality evaluation for JPEG 2000 compressed images. International Symposium on Signals, Circuits and Systems, SCS 2003, 1,137-140.

Wang, Z., Bovik, A. C., Lu, L. (2002a) Why is image quality assessment so difficult? IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '02), 4, 3313-3316.

Wang, Z., Sheikh, H. R., Bovik, A. C. (2002b) No-reference perceptual quality assessment of JPEG compressed images. Proceedings of the International Conference on Image Processing, 1, 477-480.

Yahaya, Y.H., Halip, M.H.M, Khairuddin, M.A., Maskat, K. (2010) The design of fingerprint biometric authentication on smart card for PULAPOT main entrance system," Information Technology (ITSim) International Symposium in , vol.3, no., pp.1-4

Mei, J., Sukang, l., and Xiaomei, T.(2009) "A Digital Watermarking Algorithm Based on DCT and DWT", in Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, pp. 104-107.