Visible Dual Watermarking using Wavelet Transform

Huda Naji

University of Babylon, Faculty of Information Technology, Department of Information Networks Science

halmamory@yahoo.com

Abstract

Image watermarking is widely used as a tool for copyright protection and authentication. We propose to embed two visible watermarks in a host image for enhancing protection and strength. If one of watermarks is tampered, the other watermark is used as a support to the first one. We propose three watermarking schemes called visible dual watermarking using wavelet transform; two schemes are working in wavelet domain and the other is a mixture of spatial and wavelet domains. The Proposed watermarking method is robust against attacks like DCT, DWT and JPEG compression schemes, and some geometric manipulation like image resizing.

Keywords: Watermarking; Wavelet transform; Robustness.

الخلاصة

العلامة المائية اصبحت اداة مهمة جدا لحماية الملكية الفكرية والتوثيق. تم اقتراح تقنية لاضافة علامتين مائية ظاهرة في الصورة المضيفة لتحسين الحماية والقوة بحيث انه اذا تم العبث باحدى العلامتين تستخدم العلامة الاخرى كاحتياط . نقترح في هذا البحث ثلاث تقنيات للعلامة الثنائية الظاهرة باستخدام محول المويجة، طريقتين تعمل في مجال محول المويجة والطريقة الثالثة هي مزيج من المجالين المكاني ومحول المويجة . تم تقييم طريقة العلامة المائية المقترحة باستخدام طرق ضغط مثل محول المويجة المتقطع ومحول الجيب تمام المتقطع وال JPEG . كما تم تقييم الطريقة باستخدام عملية تغيير حجم الصورة . والنتائج بينت قوة الطريقة ضد هذه العمليات.

الكلمات المفتاحية: العلامة المائية , محول المويجة ، المتانه.

1. Introduction

Most of the applications and services are prepared on-line this is why the society is a digital one. Retail services, financial services, digital libraries are examples for these applications (Topkara *et al.*, 2005).

Digital watermarks are used for a variety of applications lately, including authentication and copy protection of multimedia content. Watermarking is a process that hides the data into a multimedia object, later the watermark has been extracted as a copyright for that object which , the watermark maybe an image, audio, video, or text (Mohanty *et al.*, 2005). Figure 1 shows the generic scheme of digital watermarking.

Several techniques have been suggested recently. In general, all techniques are classified into two kinds depending on how to embed the watermark; spatial domain and transform domain. Wherein the values of image pixels are amended based on the watermark if spatial domain has been used. While in transform domain mechanisms, the image should be transformed to wavelet, DCT, or DFT then embed the watermark. Finally, the inverse transform is applied to get the watermarked image (Taskovski *et al.*, 2001). Watermarks of varying degree of visibility are added to media as a way to provide the copyright protection regardless the host data is in spatial or in transformed domains.

The main motivation of this work is based on (Taskovski *et al.*, 2001). A dual visible watermark images are embedded instead of one invisible as in (Taskovski *et al.*, 2001). In (Inamdar *et al.*, 2014), the dual watermark is proposed with multiple biometric watermarks such like speech and face biometric traits of owner invisibly, then offline signature is added on image. The scheme proposed in (Mohanty *et al.*, 1998), the secondary watermark image is embedded in the wavelet domain of a primary watermark.

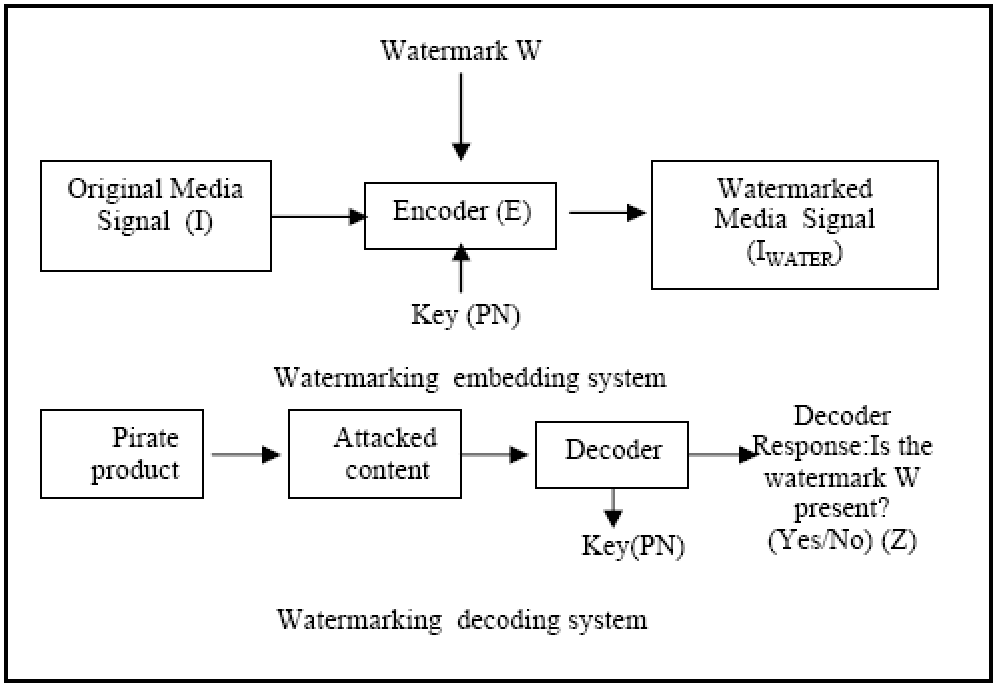

Watermark W
Original Media Signal (I)
Encoder (E)
Watermarked Media Signal (I_{WATER})
Key (PN)
Watermarking embedding system
Pirate product
Attacked content
Decoder
Decoder Response:Is the watermark W present? (Yes/No) (Z)
Key(PN)
Watermarking decoding system

Figure 1. Digital watermarking system

2. Visible Vs. Invisible Watermarks

The digital watermarks can be classified into four kinds: (i) visible watermark, (ii) invisible-robust watermark, (iii) invisible-fragile watermark and (iv) dual watermark.

A visible watermark is a secondary transparent image, which has been added to the primary image and seem a visible to viewer. As for the invisible-robust watermark, the process of embedding can be carried perceptually and can be retrieved using suitable mechanism such as decoding. With respect to the third kind, the embedding is fragile due to any manipulations in the image would damage the watermark.

On the other hand, a dual watermark is a mixture of visible and invisible watermarks, where the latter is utilized as a support for the visible watermark (Mohanty *et al.*, 2005). In this paper, a visible watermark is used as a backup for the first visible watermark.

3. Discrete Wavelet Transform (Dwt)

"Wavelets are basis functions that have some similarities to both splines and Fourier series. They have advantages when the aperiodic signal contains many discontinuities or sharp changes". Wavelets, developed in several fields; such as mathematics, statistics, and quantum physics.

The wavelet is functions, which analyzes signals into different frequency components, and analyzes each component with a resolution matching its scale.

In DWT, the image is decomposed into four frequency bands; LL, LH, HL, and HH (L=Low, H=High) as stated in Figure 2. The approximation of the original image is included in LL-sub-band while the other sub-bands contain the missing details. In the next levels, the low-pass band (LL) can be decomposed further (Youssef *et al.*, 2012).

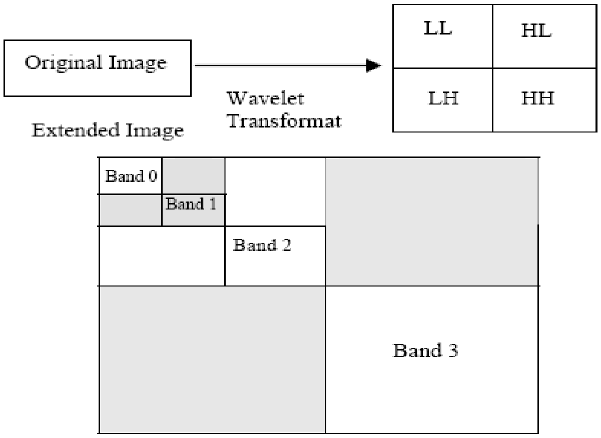


Figure 2. The wavelet coefficients at three scales

4. The Proposed Techniques of Visible Dual Watermarks

The wavelet domain can be used as a good tool for hiding the watermark. The capacity of information hiding is increased by embedding into the wavelet domain (Nafornita, 2005). It is Worth mentioning that watermarking is more difficult than steganography because the watermark should be able to survive image processing. On the other hand, in watermarking, it is possible to make the assumption that one can have an access to the original watermark and the original image (Lo. *et al.*, 1998).

The basic idea is the same in all algorithms, but it is used differently in each one. Figures 3 and 4 show the original test and watermark images used in this experiment.

4.1. Visible dual watermark algorithm 1. (A. 1)

In this work, the original image and the watermark are first decomposed using the wavelet pyramid structure for two levels. Then, the wavelet coefficients W_W, of the low-resolution representation (LL) of the watermark W, are embedded in the coefficients I_W of the low-resolution representation of the original image I and other coefficients (LH, HL, and HH) of the watermark image are embedded in the higher frequency components of the image I, which represents the edges and textures of the image,as follows:

$$I_W' = I_W + \alpha W_W \dots (1)$$

Where α is a scale factor .Using (1), one of the dual watermarks is embedding in first level, and the other one is embedding in the second level. Thus, the watermarked image is obtained by applying the invers discrete wavelet transform (IDWT) to $I'w$.

In this work, the coefficients of low-resolution representation of the watermarked image has been embed the same way the coefficients of high-resolution representation are done. This is the main difference between this work and that proposed in (Taskovski *et al.,* 2001). Figure 5 shows the application of the algorithm (1) on images are shown in figure 3((a),(b)).

4.2. Visible dual watermark algorithm 2. (A. 2)

The proposed technique here is the same as in first algorithm. Instead of inserting one watermark in each level, the dual watermarks are inserted at one time and in one level of decomposition. So (1) is modulated as:

$$I_W^{\prime} = I_W^{\prime} + \alpha W1_W + \beta W2_W \ldots (2)$$

Where α, β are scale factors, and $W1_W$,$W2_W$ are dual watermarks. Figure 6(a) shows the application of the algorithm (2) on image shown in figure 3(a).

4.3. Visible dual watermarks algorithm 3. (A. 3)

Image In this subsection, a mixture of special and wavelet domains is suggested. In the special domain, the same technique used in (Mohanty *et al.,* 2005) is followed. The watermarked image is acquired by adding a scaled gray value of the watermark image to the host image as follows:

$$I^{\prime}(m,n) = \begin{cases} I(m,n) + \left(\frac{\alpha_I}{6.0976}\right) W(m,n) I(m,n)^{\frac{2}{3}} \\ \quad for\ I(m,n) > 2.2583 \\ I(m,n) + \left(\frac{\alpha_I}{903.3}\right) W(m,n) I(m,n) \\ \quad for\ I(m,n) \le 2.2583 \end{cases} \ldots (3)$$

Where α_I is a global scaling factor. The watermarked image I′(m,n) resulting by using (3) is decomposed in the wavelet domain for one level to insert the other watermark by using (1) . Figure 6(b) shows the application of the algorithm (3) on image shown in figure3(a**).**

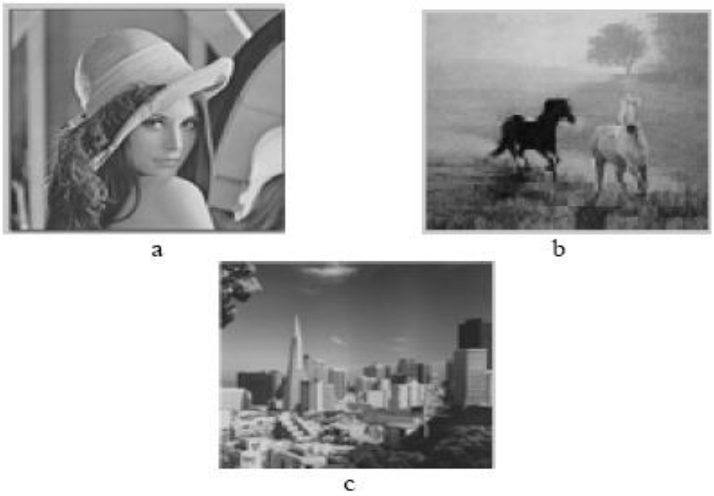


Figure 3. Original Host Images (a, b, and c)

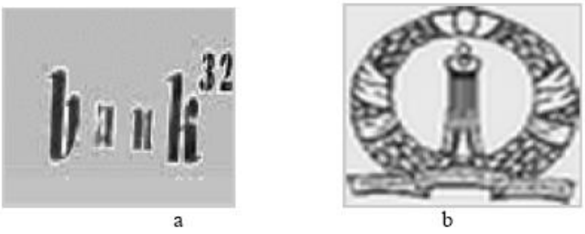


Figure 4. Original watermark Images (a, b)

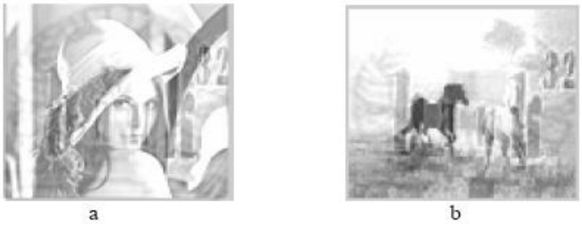


Figure 5. Watermarked Images for the first algorithm (α_{level1}=0.15 and α_{level2}=0.4)

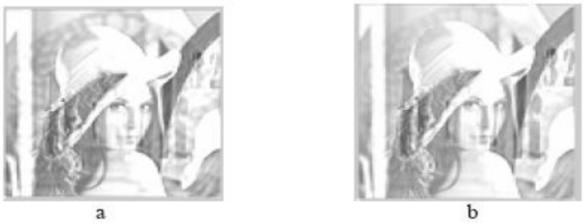


Figure 6. Watermarked images for the a) second algorithm (α=0.1 and β=0.4) b) third algorithm (α_1=0.3, α=0.4)

5. Watermark Detection

The marking algorithm must have a sufficient detection capability (low probability of false alarm and high probability of detection) for data to be inserted. The detection performance is affected by the length of the data inserted, mark redundancy, and the size of the stream in which the mark is inserted. In a piece of content of a given size, a short mark might be inserted many times to achieve a high recovery probability, whereas long marks can be inserted a few times only, potentially degrading recoverability (Lacy *et al.*, 1998) . Generally, the correlation techniques are used as kind of watermark detection, so long as there is no across correlation between the watermark and the cover image so that means that work is good. However, the main problem in this area is that watermark prepared independent of the cover image. Therefore, the probability of finding cross correlation is high. Subtracting the original image before extracting the watermark is considered the solution for this problem. Whereas other works suggest pre filter as a solution for that problem (Muharemagic *et al.,* 2004).

The problem of detection is mostly carried out in the same domain of creating and embedding the watermark.

In the wavelet domain, the coefficients of the low and high-resolution representations of the extracted watermark are obtained as (D. Taskovski. et al., 2001):

$$\overline{W}_w = \frac{1}{\alpha}[\bar{I}_w - I_w] \dots (4)$$

With IDWT of $\overline{W}_w$ for two levels, the extracted dual watermark $\overline{W}$ is obtained. Figure 7 shows the extracted watermarks. Since, we use visually recognizable pattern as watermark, extracted watermarks can be compared with original watermarks subjectively. Besides subjective judgment for the watermark fidelity, we have used an objective measure of correlation between the original watermark and the extracted one. Table 1 shows the correlation between the two-extracted watermark and the original images (MATLAB function “corr2"is used).

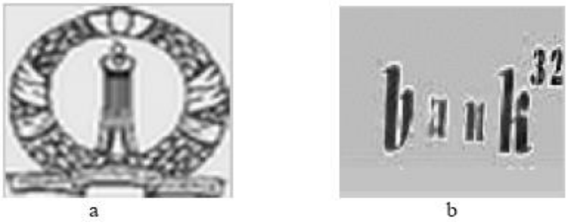
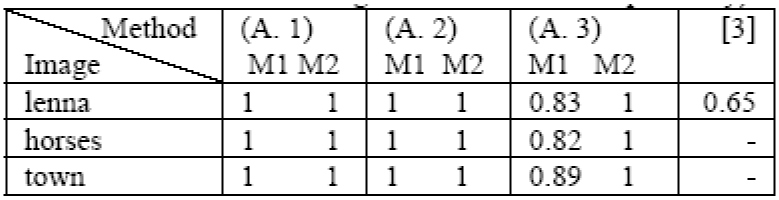


Figure 7. The two extracted watermark images from watermarked image shown in figure 5. (a)

Table 1. Show the correlation for M1 and M2 (the first extracted watermark images and the second respectively)



Method Image	(A. 1) M1	 M2	(A. 2) M1	 M2	(A. 3) M1	 M2	[3]
lenna	1	1	1	1	0.83	1	0.65
horses	1	1	1	1	0.82	1	-
town	1	1	1	1	0.89	1	-

6. Robustness

Digital images usually undergo several kinds of attacks, such as filtering, compression, rotation, resizing, and contrast enhancement. The watermark is robust if it is extracted even after exposed to attacks. However, if the watermark embeds in perceptually important portions of the image leads to resist the distortions. In this section, some of the schemes used in (Taskovski *et al.,* 2001) for proving the robustness are also used here**.** The compression is a commonly operation applied on images. Therefore, resistance to this operation is a good test for watermarking robustness (Taskovski *et al.*, 2001). Worth to mention, resistance to geometric manipulations are still an open issue. Regarding resizing, MATLAB function “imresize” is used by applying bicubic method. The schemes of compression for watermarked image are DCT, DWT and JPEG. Regarding DWT, MATLAB function “wdencmp” is used to compress a watermarked image. Extracted watermarks are shown in figures 8 and 9. Table 2 shows the correlation between the two-extracted watermark and the original images.

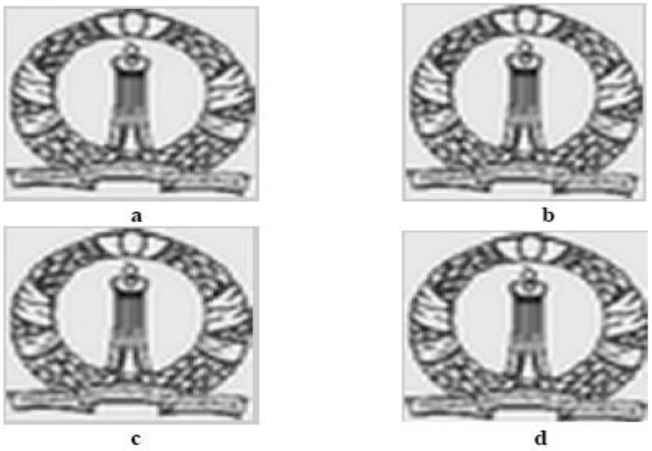
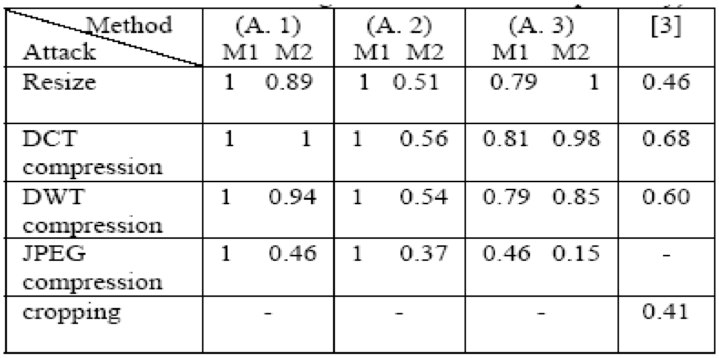


Figure 8. The first extracted watermark image from watermarked image shown in Fig. 5. a (a) rescaled reduction \ enlargement is done (b)DCT compressed (c)DWT compressed (d) JPEG compression.

Table 2. Show the correlation for M1 and M2(the first extracted watermark images and the second respectively)



Method / Attack	(A. 1)		(A. 2)		(A. 3)		[3]
	M1	M2	M1	M2	M1	M2	
Resize	1	0.89	1	0.51	0.79	1	0.46
DCT compression	1	1	1	0.56	0.81	0.98	0.68
DWT compression	1	0.94	1	0.54	0.79	0.85	0.60
JPEG compression	1	0.46	1	0.37	0.46	0.15	-
cropping	-		-		-		0.41

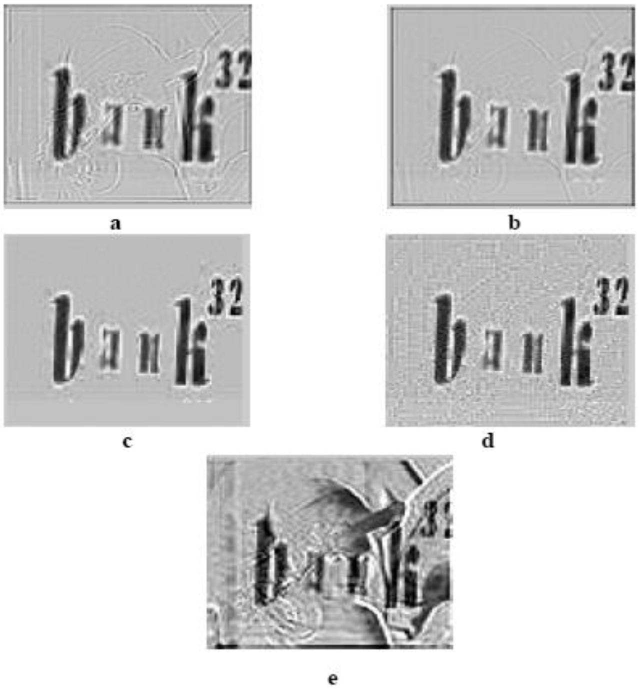


Figure 9. The second extracted watermark image from watermarked image shown in Fig. 5. a (a) where 25% reduction (b)where 50% enlargement (c) DCT compressed (d) DWT compression (e) JPEG compression.

7. Conclusion

In this paper, a watermarking technique is presented called visible dual watermarking based wavelet. The dual watermark serves as it establishes the owner's right and detects the tampering of the image. A multiresolution nature of wavelet transform serves as a good tool for embedding more than one watermark image. On the other hand, the proposed scheme has proved it is robust against DCT, DWT and JPEG compression schemes, and some geometric manipulations like image resizing. The first watermark is more robust than the second in algorithms 1 and 2. In algorithm 3, the second watermark be more robust than the first, but this is not applied to JPEG compression where the first watermark is more robust than the second. In general, the proposed scheme is more robust than that proposed in (Taskovski *et al.,* 2001) as shown in Table 2.

8. References

Inamdar, V. S.; P. Rege, 2014," Dual watermarking technique with multiple biometric watermarks", Sadhana, Vol. 39, pp.3-26.

Lacy, J.; S. Quackenbush, and A. Reibman, 1998, "Intellectual property protection systems and digital watermarking", Journal of Optics Express, vol. 3, pp. 478 -484.

Lo, H.Y.; S. Topiwala, and J. Wang, 1998" Wavelet Based Steganography and watermarking", http://www.cs.cornell. edu/topiwala/wavelets/report.html.

Mohanty, S.P.; N. Ranganathan, and R. K. Namballa, 2005,"A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S2DC) Design" , IEEE

Transaction on Very Large Scale Interation (VLSI)Systems, Vol.XX, No.Y , http://citeseer . ist.psu.edu /cache /papers /cs2 /522/http:zSzzSzwww.cs.unt.eduzSz~smohantyzSzresearchz Sz JournalPaperszSz2005zSzMohantyTVLSI2005SpatialVisWM.pdf/mohanty05vlsi.pdf.

Muharemagic, E.; B. Furht, 2004, "Multimedia Security: Watermarking Techniques" http://www.cse.fau.Edu/~borko/MulChapter,%20Watermarking%20IEC2004.pdf.

Nafornita, C. 2005, " Digital Watermarking in the Wavelet Domain", Politehnica Publishing House, Timisoara, 42pages, ISBN 973-625-236-1.

Sharkas, M.; D. ElShafie, and N. Hamdy, 2005, “A Dual Digital- Image Watermarking Technique", In Proc. of 3rd World Enformatika Conference, 136-139.

Taskovski, D.; S. Bogdanova, and M. Bogdanov, 2001," Digital watermarking in Wavelet Domain", International symposium on image and signal processing and analysis N^{o}2, Pula, CROATIE, pp. 604-608.

Topkara, M.; A. Kamra, and M. J. Atallah, 2005, " ViWiD: Visible Watermarking based Defense against Phishig", lectures notes on computer science, "Digital watermarking" Vol. 3710/2005, 4th International Workshop, IWDW 2005, Siena, Italy, Proceedings.

Youssef, S. M.; S. Mesbah ,and Y. M. Mahmoud,2012, "A Hybrid Wavelet-based Image Retrieval ", Journal of Next Generation Information Technology (JNIT), Vol. 3,No. 3.