A Hybrid Image Cryptographic and Spatial Digital Watermarking Encryption Technique for Security and Authentication of Digital Images

Quist-Aphetsi Kester[124], Laurent Nana[2], Anca Christine Pascu[3], Sophie Gire[2],Jojo M. Eghan[4], Nii Narku Quaynor[4]
[1]Faculty of Informatics, Ghana Technology University College, Accra, Ghana
kquist-aphetsi@gtuc.edu.gh / kquist@ieee.org
[2]Lab-STICC (UMR CNRS 6285), European University of Brittany, University of Brest, France
[3]HCTI EA 4249 and Lab-STICC (UMR CNRS 6285) European University of Brittany, UBO, France
[4]Department of Computer Science and Information Technology, University of Cape Coast, Cape Coast, Ghana

Abstract— **The digital image data transmission and storage in today's cyberspace has increase with privacy and security concerns. Digital media collected from different sources such as surveillance systems, forensic databases, medical images are very sensitive hence security concerns regarding the safe transmission and authentication of such digital data across secured and unsecured communication channels needs to be addressed. This security to such images should be easily used to identify the source, detect modification and secure the content of the image as well as avoiding pixel loss during the original image recovery process. In this paper, we proposed a hybrid image cryptographic encryption and digital watermarking technique for the encryption and authentication of digital image content. The image encryption was done on the RGB channels and the spatial watermarking was successfully applied to the RGB-colour bands of the digital image and this rendered the watermark visibly subtle and difficult to detect under regular viewing. The digital watermarking technique was engaged to authenticate the image and detect modifications to the watermarked image. The watermark visibility and detection was difficult to detect and the image was successfully reconstructed without any loss of pixel value after decryption. The programming and implementation was done using MATLAB.**

Keywords- Cryptography, digital image, Encryption, Watermarking, pixel, authentication

I. INTRODUCTION

Security and privacy are the dominant needs in the current information age where massive usage of cloud systems and transmission of huge multimedia contents are concerned. With the rapid growth and dependence on usage of mobile applications, there is a need for easily implementable but robust security features in multimedia contents [1]. This will aid in copyright and ownership issues as well as forensics investigative processes making easy to trace source as well as to detect temperament.

The existence of security of communication can be traced to the early days in BC such as Julius Caesar and it has transformed overtime from classical to modern approaches and has dominated the digital with its usage in every day internet transactions [2]. This has evolved from classical symmetric [3] to modern symmetric ciphers [4] and then to modern public key exchange cryptosystems [5]. Now there are advancements in key exchange using Quantum cryptography [6] as well as post quantum cryptography [6]. Some examples of these algorithms are RSA, ElGamal, elliptic curve, Diffie-Hellman key exchange[7], and they are used in digital signature algorithms and now cutting edge works such as the quantum cryptography [8][9].

Watermarking approaches [10] are used in applications for authentication, validation of copyright ownership, broadcast monitory, source tracking etc [11]. It is accomplished by embedding and hiding some authenticated piece of information behind the digital data such as an image, audio or the video file [12]. This hidden data is then used to verify ownership, authenticity etc. of the transmitted data. To achieve a higher detection of temperament or malicious modification of the carrier signal, a hybrid approach of cryptographic and watermarking techniques can provide a good solution.

This paper proposed a hybrid cryptographic and digital watermarking technique for securing digital images. The RGB channels of the digital image were utilized for both approaches. The watermarking technique was used to authenticate the image whilst the cryptographic technique protects the content of the image. The paper has the following structure: section II Related works, section III Methodology, section IV The explanation of the procedure used, section V results and analysis, and section VI concluded the paper.

II. RELATED WORKS

Digital watermarking, Steganography and cryptography are key areas of data security and information hiding. These techniques have become very important in a number of application areas [13]. ShunDa Lin, in his paper proposed a new method of image transmission and cryptography on the basis of Mobius transformation. Based on the Mobius transformation, the method of modulation and demodulation in Chen-Mobius communication system, which was quite different from the traditional one, was applied in the image transmission and cryptography. In achieving such a processing, the Chen-Mobius inverse transformed functions act as the "modulation" waveforms and the receiving end is coherently "demodulated" by the often-used digital waveforms. From his results, it was established that his new applications had excellent performances that the digital image signals can be restored from intense noise and encrypted ones [14]. Jiang Hua et al proposed a solution of

978-1-4799-8713-9/15 $31.00 © 2015 IEEE
DOI 10.1109/UKSim.2015.85

video semi-fragile watermarking of authentication based on binary characteristic strings. In the work, the binary characteristic string was obtained from I-frame by using the semi-fragile characteristic and the binary watermarking was generated by using the properties string as the encryption key and at the end, the integrity of MPEG-4 videos' I-frame was protected and authenticated [15]. Watermarks that work on RGB channels ended up modifying luminance. Huang, P.S et al in their work proposed a novel and robust colour watermarking approach for applications in copy protection and digital archives and was is computationally efficient. Their scheme successfully makes the watermark perceptually invisible and robust to image processing operations such as general image processing operations (JPEG2000, JPEG-loss compression, lowpass filtering, and medium filtering), image scaling and image cropping [16]. Musheer Ahmad and Tanvir Ahmad in their work also proposed an efficient ciphering approach to secure the multimedia colour imagery. Complex dynamic responses of multiple high-order chaotic systems were utilized to carry out image pixels shuffling and diffusion processes under the control of secret key. The pixels diffusion was done by randomly picking the actual encryption keys out of nine hybridized keys that were extracted from complex sequences of Chen, Rossler and Chua chaotic systems. The shuffling and diffusion processes made plain-image information dependent to resist the potential chosen-plaintext, chosen-ciphertext and known-plaintext attacks [17]. For biometric applications and devices gathering sensitive data for analysis such as public surveillance policing systems, Kester, Quist-Aphetsi, et al, proposed a hybrid encryption technique for securing biometric image data based on Feistel Network and visual cryptography [18]. Cryptography is a vital technique to keeping private data secretly in order to avoid unauthorized access and also to ensure data integrity. Cryptographic schemes make use of encryption methods such as DES, RSA etc... Chaotic encryption of an image encryption scheme in which shifting the positions and changing the grey values of image pixels are combined simultaneously to ensure a high level of security was proposed by Dongming Chen. Arnold cat map was used to permute the positions of the image pixels in the spatial domain. Then another chaotic logistic map was used to substitute the relationship between the ciphered image and the original image. An external 128 bit secret key was employed and was further modified after encrypting each pixel of the original image to make the encryption more robust against attacks. Sensitivity analysis, key space analysis and statistical analysis of several experimental results were feasible [19].

In this paper, a hybrid image cryptographic and digital watermarking encryption technique for encryption digital image content and authentication was proposed. The RGB channel bands of the digital image were used and this rendered the watermark visibly subtle and difficult to detect under regular viewing. The digital watermarking technique was engaged to authenticate the image and detect modifications to the watermarked image.

III. METHODOLOGY

The method of implementation consists of the image cryptographic phase and the watermarking process. The cryptographic approach used visual image encryption technique as well as pixel displacement. A sequential embedding technique was engaged in the implementation process of the watermarking. This proposed approach was implemented on nxm size of plain image. There was no pixel expansion during the encryption process but there was a change in pixel position. There was a change in pixel values after the application of the watermark but during the decryption phase, the watermark was removed and the pixel was restored. This makes the entire process suitable for situations that depends on fully recoverable image after encryption and watermarking processes. During the encryption process certain features of the image was used and the remained constant for both the plain image and the ciphered image but not for the watermarked image. The features engaged were the entropy, the arithmetic mean and the nth value of the row and column count of both the plain and the ciphered images. The implementation was done using MATLAB.

Figure 1 below showed the summary of the cryptographic and watermarking process used in the ciphering process of the digital plain image. Where PI is the plain image and CI is the ciphered image. Alg(PI,β,α) is the algorithm used in the embedding of the watermark and ciphering process.

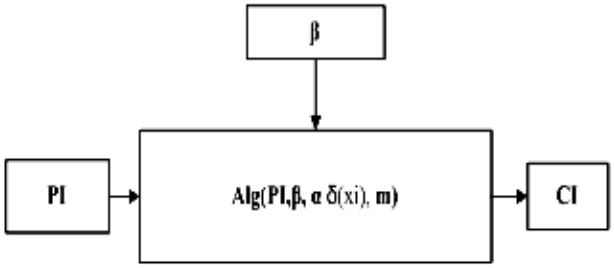

Figure 1. The summary of the processes engaged.

β=message to be embedded
α =symmetric encryption key used for the pixel encryption.
f(PI)=symmetric key generated from the plain image
$\bar{x}$ = m = arithmetic mean. It calculates the arithmetic mean of a the plain image, watermarked and ciphered images. x=pixel value and n = the total number of pixel values.
The arithmetic mean is

$$\overline{X} = \frac{\sum_{i=1}^{n} X_i}{n} \quad (1)$$

δ(xi) = entropy(I) returns the Entropy of the plain image, wartermarked image or ciphered images, which is a scalar value representing the entropy of grayscale image I. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image.

Entropy is defined as δ(i))=-sum(xi.*log2(xi)) (2)

Ÿ(xi) was computed to return the index value of the arithmetic mean of the plain, watermarked and ciphered images with respect to the total entropy of the RGB image.

$$Ÿ(xi) = m(xi) / \Sigma((xi=\{R,G,B\}))) \quad (3)$$

Ψ (xi) was computed to return the index value of the entropy of the plain, watermarked and ciphered images with respect to the total entropy of the RGB image.

$$\Psi(xi) = \delta(xi) / \Sigma((xi=\{R,G,B\}))) \quad (4)$$

IV. THE TECHNIQUES ENGAGED

The explanations for the approaches used consisted of the image encryption and the process.

A) The computing the feature constant

Fk was generated from the plain image, PI, based on certain features of the image and it is as below.

$$Fk = [(c \times p) + |(\delta(xi)| + |(m = (1/n) . \sum_{i=1}^{n} x_i)|] \bmod p \quad (5)$$

c= nth row value
P= nth column value

B) The image encryption process.

The image encryption process engaged *Fk* in ciphering the image and displacing the pixel values using a visual cryptographic technique.

Start
Let PI= f (R, G, B)
new_image=imread(PI);
PI is a color image of m x n x 3 arrays
(R, G, B) = m x n
Where R, G, B ∈PI
(R o G) i j = (R) ij. (G) ij
Where r_11 = first value of R
r= [ri1] (i=1, 2… m)
x r_i1 : [a, b]= {x ∈ I: a ≤ x ≥ b}
a=0 and b=255
R= r= PI (m, n, 1)
Where g_12 = first value of G
g= [gi2] (i=1, 2... m)
x ∈ g : [a, b]= {x ∈ I: a ≤ x ≥ b}
a=0 and b=255
G= g= PI (m, n, 1)
And b_13 = first value of B
g= [bi3] (i=1, 2... m)
x ∈ b_i1 : [a, b]= {x ∈ I: a ≤ x ≥ b}
a=0 and b=255
B=b=PI (m, n, 1)
for i: Δi:*Fk*
Let *t'(i,j)* =Transpose of r(i,j)=r
t'(i,j)= f(r',c,p);
Let *y'(i,j)* =Transpose of b(i,j)=g
y'(i,j)= f(g',c,p);
Let *u'(i,j)* =Transpose of u(i,j)=b
u'(i,j)= f(b',c,p);
end
Transformion of *t'(i,j) into f(t'(i,j)*,c,p))
r= f(t'(i,j),c,p))*=f(r, c, p)*
Transformion of *y'(i,j)into f(y'(i,j)*,c,p))
g= f(y'(i,j),c,p))*=f(g, c, p)*
Transformion of *u' (i,j) into f(u'(i,j)*,c,p))
b= f(u(i,j),c,p))*=f(b, c, p)*
CI= f (3,r,g,b);
end

C) Implementation of the Watermarking

The following approach was used to embed the data into the image.

R=f (:,:,1); is the separation of the red channel as 'r'
Let (:,:,1)=size of R be m x n [row, column]
size (R) = R (m x n)
rij= r=CI (m, n, 1)
g=f (:,:,2); is the separation of the green channel as 'g'
Let (:,:,2)=size of G be m x n [row, column] = size (G)
gij= g= CI (m, n, 1)
b=f (:,:,3); is the separation of the blue channel as 'b'
Let f (:,:,3);=size of B be m x n [row, column]
size (B) = B (m x n)
bij= b= CI (m, n, 1)
[c, p]=s(r); is the size of r as [c, p]
Let s(r) =size of R be [row, column] = size (r) =r (c x p)
Embedding the data into CI
d=Aij, where d is the data to be embedded
x ∈Aij : [a, b]={x ∈ I: a ≤ x ≥ b}where a=0 and b=255
Let the size of d be [c1, p1]=size(d);
Let λ=x_i : x_i∈ I: 0 ≤ x ≥ ∞;
Let η=x_i : x_i∈ I: 0 ≤ x ≥ ∞;
for i=1:1:c1
for j=1:1:p1
if((i== λ)&& (j== η))
t(i,j)=(Aij+ t(i,j)) mod 256;
y(i,j)=g(i,j);
u(i,j)=b(i,j);
λ = λ +Δ λ ;
η = η +Δ η ;
if(c1>c)
t(i,j)=r(i,j);
y(i,j)=g(i,j);
u(i,j)=b(i,j);
if(p1>p)
t(i,j)=r(i,j);
y(i,j)=g(i,j);
u(i,j)=b(i,j);
else
end
else
t(i,j)=r(i,j);
y(i,j)=g(i,j);
u(i,j)=b(i,j);
end
end
end

V. SIMULATED RESULTS AND ANALYSIS

The image below was encrypted and analyzed using the proposed approach and this was implemented in MATLAB. The recovery of the plain image from the watermarked ciphered image was achieved successfully.

Figure 2. The plain image : obtained from a surveillance micro UAV.

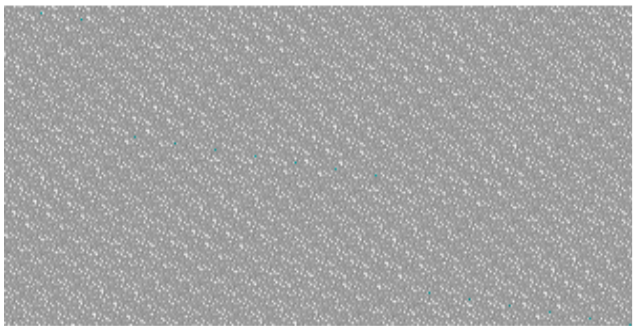

Figure 3. The ciphered and watermarked image of figure 2.

The plain image in figure 2 above is the mxn image used for the encryption process and Figure 3 is the result of the ciphered and watermarked image.

TABLE 2: ANALYSIS OF PLAIN, CIPHERD WATERMARKED AND IMAGE.

xi	*m*	δ(xi)	Ÿ(xi)	Ψ (xi)
PI(R)	163.3301	5.7878	0.333273	0.333333
PI(G)	163.3744	5.7878	0.333363	0.333333
PI(B)	163.3744	5.7878	0.333363	0.333274
CI(R)	163.3301	5.7878	0.333273	0.333333
CI(G)	163.3744	5.7878	0.333363	0.333333
CI(B)	163.3744	5.7878	0.333363	0.333333
WI(R)	163.3301	5.7909	0.333273	0.333512
WI(G)	163.3744	5.7878	0.333363	0.333274
WI(B)	163.3744	5.7878	0.333363	0.333274

The table above consist of the mean *m*, entropy δ(xi). Ÿ(xi) was computed to return the index value of the arithmetic mean of the plain, watermarked and ciphered images with respect to the total entropy of the RGB image. Ψ (xi) was computed to return the index value of the entropy of the plain, watermarked and ciphered images with respect to the total entropy of the RGB image.

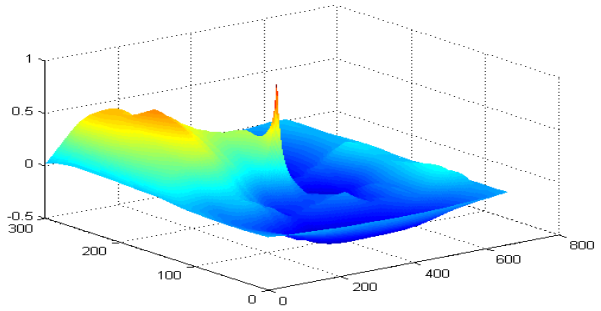

Figure 4. The graph of the normalized cross-correlation of the matrices of the ciphered image.

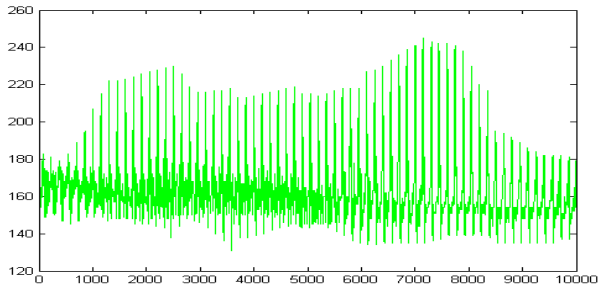

Figure 5. The graph of the first 10000 pixel value of figure 2 .

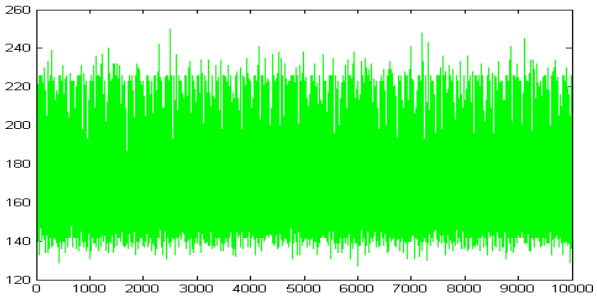

Figure 6. The graph of the first 10000 pixel value of figure 3 .

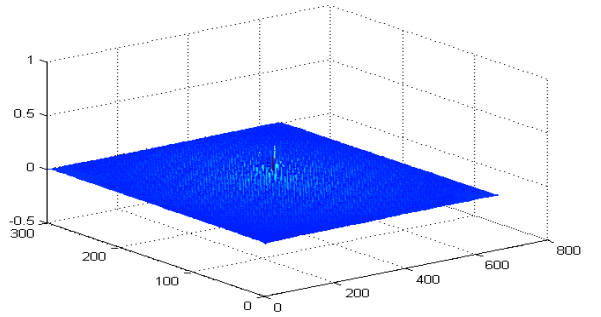

Figure 7. The graph of the normalized cross-correlation of the matrices of the ciphered image.

The normalized cross-correlation of the matrices of is

$$\gamma(u,v)=\frac{\sum_{x,y}\left[f(x,y)-\bar{f}_{u,v}\right]\left[t(x-u,y-v)-\bar{t}\right]}{\left\{\sum_{x,y}\left[f(x,y)-\bar{f}_{u,v}\right]^2\sum_{x,y}\left[t(x-u,y-v)-\bar{t}\right]^2\right\}^{0.5}} \quad (6)$$

f is the mean of the template, $\bar{t}$ is the mean of in the region under the template. $\bar{f}_{u,v}$ is the mean of $f(u,v)$ in the region under the template.

VI. CONCLUSION

Water marking in spatial domain embeds the data directly into the pixel data making it semi fragile approach and they alter the host image during embedding phase. Further they have the lowest bit capacity and the lowest resistance to JPEG compression. But they are very effective to detect temperament or malicious attack on them. The approach is effective because the watermark can be extracted and the image can easily be recovered without pixel expansion or data loss. The invisibility of the watermark approach will make it difficult for detection and hacking.

This proposed approach is suitable for effective watermark authentication and applications in which full recovery of image content is necessary after deciphering of the ciphered image and removal of watermarks. It will be useful in applications such as medical images stored in the cloud, military communication networks where authentication of visuals is crucial for example, Unmanned Aerial vehicles, video surveillance systems, satellite communication systems etc.

ACKNOWLEDGMENT

This work was supported by Lab-STICC (UMR CNRS 6285) at UBO France, AWBC Canada, Ambassade de France-Institut Français-Ghana and the DCSIT-UCC, and also Dominique Sotteau (formerly directeur de recherche, Centre national de la recherche scientifique (CNRS) in France and head of international relations, Institut national de recherche en informatique et automatique, INRIA) and currently the Scientific counselor of AWBC, Canada.

REFERENCES

[1] Seong-Yeon Lee; Kwang-Seok Moon; Jong-Nam Kim, "Implementation of Real Time DMB Encryption on PMP for Copyright Protection," Convergence and Hybrid Information Technology, 2008. ICCIT '08. Third International Conference on , vol.2, no., pp.446,449, 11-13 Nov. 2008doi: 10.1109/ICCIT.2008.320

[2] Song Y. Yan. 2013. Computational Number Theory and Modern Cryptography (1st ed.). Wiley Publishing.

[3] William, S., & Stallings, W. (2006). Cryptography and Network Security, 4/E. Pearson Education India.

[4] Forouzan, B. A. (2007). Cryptography & Network Security. McGraw-Hill, Inc..

[5] Diffie, W. (1988). The first ten years of public-key cryptography. Proceedings of the IEEE, 76(5), 560-577.

[6] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of modern physics, 74(1), 145.

[7] Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-quantum cryptography. Springer Science & Business Media.

[8] Kester, Q.-A.; Nana, L.; Pascu, A.C., "A novel cryptographic encryption technique of video images using quantum cryptography for satellite communications," Adaptive Science and Technology (ICAST), 2013 International Conference on , vol., no., pp.1,6, 25-27 Nov. 2013 doi: 10.1109/ICASTech.2013.6707496

[9] Chip Elliott, David Pearson, and Gregory Troxel. 2003. Quantum cryptography in practice. In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '03). ACM, New York, NY, USA, 227-238. DOI=10.1145/863955.863982 http://doi.acm.org/10.1145/863955. 863982

[10] Bhattacharya, S., Chattopadhyay, T., & Pal, A. (2006, June). A survey on different video watermarking techniques and comparative analysis with reference to H. 264/AVC. In Consumer Electronics, 2006. ISCE'06. 2006 IEEE Tenth International Symposium on (pp. 1-6). IEEE.

[11] Nin, J., & Ricciardi, S. (2013, March). Digital watermarking techniques and security issues in the information and communication society. In Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on (pp. 1553-1558). IEEE.

[12] Kumar, M.; Hensman, A., "Robust digital video watermarking using reversible data hiding and visual cryptography," Signals and Systems Conference (ISSC 2013), 24th IET Irish , vol., no., pp.1,6, 20-21 June 2013 doi: 10.1049/ic.2013.0051

[13] Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. Proceedings of the IEEE, 87(7), 1062-1078.

[14] ShunDa Lin, "Image transmission and cryptography on the basis of Mobius transform," Image and Signal Processing (CISP), 2012 5th International Congress on , vol., no., pp.258,261, 16-18 Oct. 2012 doi: 10.1109/CISP.2012.6469901

[15] Jiang Hua; Wang HuiJiao; Wang Xin, "A Solution of Video Semi-fragile Watermarking of Authentication Based on Binary Characteristic Strings," Multimedia Information Networking and Security, 2009. MINES '09. International Conference on , vol.2, no., pp.167,170, 18-20 Nov. 2009doi: 10.1109/MINES.2009.27.

[16] Huang, P.S.; Chiang, C.-S.; Chang, C.-P.; Tu, T.-M., "Robust spatial watermarking technique for colour images via direct saturation adjustment," Vision, Image and Signal Processing, IEE Proceedings - , vol.152, no.5, pp.561,574, 7 Oct. 2005doi: 10.1049/ip-vis:20041081

[17] Musheer Ahmad and Tanvir Ahmad. 2014. Securing multimedia colour imagery using multiple high dimensional chaos-based hybrid keys. Int. J. Commun. Netw. Distrib. Syst. 12, 1 (November 2014), 113-128. DOI=10.1504/IJCNDS.2014.057991 http://dx.doi.org/1 0.1504 /IJCNDS.2014.057991

[18] Kester, Quist-Aphetsi, et al. "A Hybrid Encryption Technique for Securing Biometric Image Data Based on Feistel Network and RGB Pixel Displacement." Recent Trends in Computer Networks and Distributed Systems Security. Springer Berlin Heidelberg, 2014. 530-539.

[19] Dongming, Chen, "A Feasible Chaotic Encryption Scheme for Image," Chaos-Fractals Theories and Applications, 2009. IWCFTA '09. International Workshop on , vol., no., pp.172,176, 6-8 Nov. 2009 doi: 10.1109/IWCFTA.2009.43