International Journal of Security and Its Applications
Vol.9, No.1 (2015), pp.409-418
http://dx.doi.org/10.14257/ijsia.2015.9.1.39

Joint Fingerprinting/Encryption for Medical Image Security

Conghuan Ye, Zenggang Xiong*, Yaoming Ding, Xueming Zhang, Guangwei Wang, and Fang Xu

College of Computer and Information Science, Hubei Engineering University, Xiaogan, Hubei, China
xzg@hbeu.edu.cn

Abstract

Electronic health records (EHRs) facilitates the healthcare process. However, it can also cause serious security and privacy problems. While various conventional encryption mechanisms can solve some aspects of these problems, they cannot address the illegal distribution of decrypted medical images. To protect decrypted medical images from being illegally distributed by an authorized staff member, the scheme proposed in this paper provides a joint fingerprinting and encryption (JFE) scheme based on GoL (Game of Life) and DNA computing with the purpose of protecting medical media distribution. In this study, GoL and DNA are used to confuse in DWT domain and diffusion in spatial domain respectively, and fingerprints are embedded into the HL and LH subbands of DWT domain. The use of fingerprinting along with encryption can provide a double-layer of protection to medical image. Experimental results show the effectiveness of the proposed scheme.

Keywords: *fingerprinting, encryption, EHRs, medical image security*

1. Introduction

EHRs (electronic health records), which is defined as a systematic collection of electronic health information about individual patients or populations, may include a range of data, such as demographics, medical history, medication and allergies, immunization status, laboratory test results, laboratory and radiologic reports, vital signs, personal stats like age and weight, billing information and medical image [1]. A number of benefits can be achieved with EHRs, the widespread use of EHRs is inevitable. However, inevitability does not mean easy transition. Concerning about on privacy and security of medical information may limit use. Therefore, wide dissemination of EHRs requires maintaining patient privacy and security protection [2].

Medical records that are exchanged over the Internet are subject to the same security and privacy threat posed by the interoperability of a national network as any other type of data transaction over the Internet [3]. Transmitting medical images between hospitals and exchanging the patients' data such as images and diagnostic reports between physicians via networks pose new challenges for protecting privacy [4, 5]. Thus, comprehensive principles concerning medical information security[6] as well as patient privacy are necessary for every participant [7]. A popular method is selective encryption. Unfortunately, these encryption algorithms have a potential security drawback [8]: the significant coefficients that are not encrypted are likely to reveal information in the original images. And there is another security vulnerability that has not been considered by these schemes, when the ciphered data is deciphered by the authorized user, it is unprotected.

Actually, encrypted data need an additional level of protection. The authors proposed a specific multicast fingerprinting solution based on the digital watermarking mechanism.

ISSN: 1738-9976 IJSIA

Therefore, the illegal distribution of the medical image can be tracked by extracting the watermark message [2, 9-11]. Since none of encryption and watermarking alone can provide the protection. D. Bouslimi *et al.*, proposed a joint encryption/watermarking algorithm for medical images based on the merging of a stream cipher algorithm (RC45) and watermarking approaches in [12], in this model, the malicious staff member can be tracked by a watermarked clue. Encryption and watermarking technologies are both advancing rapidly, creating opportunities for EPRs security. The convergence of the two technologies is now facilitating privacy and security studies. In[12], encryption and watermarking are considered together to trace medical data during its distribution.

On the other hand, CA (Cellular automata) is capable of developing chaotic behavior using simple operations or rules offering the benefit of high speed computation. The ability to obtain complex global behavior makes CA an interesting platform for digital image scrambling [13-16]. Fast computation helps in achieving this capability. At the same time, DNA cryptography [17, 18] is born as a new cryptographic field emerged, DNA computing has been found lots of good characteristics such as massive parallelism, huge storage and ultra-low power consumption [19].

In practice, permutation and diffusion are often combined in order to get high computational security. A new JFE (joint fingerprinting/encryption) algorithm based on GoL and DNA computing in hybrid domains is proposed. This algorithm is simple, secure, fast and easy to be realized, which is suitable for encrypting medical images. This research provides a substantial contribution to high-speed implementation and information security of medical image. Above all, the proposed scheme can continually protect decrypted medical images from being illegally distributed by an authorized staff member. Therefore, by combining fingerprinting and encryption mechanisms the risk of the illegal distribution of authorized users can be reduced using the proposed scheme.

2. Basic Theory of the Proposed Scheme

2.1. DNA Computing

In 1994, Adleman [19] did the first experiment of DNA computing. Single-strand DNA sequence contains four nucleic acid bases $A(adenine)$, $T(thymine)$, $C(cytosine)$, $G(guanine)$, where A and T are complementary, so are C and G. Four bases A, C, G and T can encode 00, 01, 10 and 11. For example, if the first pixel value of the medical image is 141, convert it into a binary sequence is [10001101]. By using a DNA encoding Rule to encode it, we can get the DNA sequence [CATG].

2.2. Cellular Automata

CA [13] are dynamical complex space and time discrete systems. The (2-D) CA called the GoL, which consists of an $[M \times N]$ matrix of cells, where each cell may take only two states: alive and dead (respectively represented by one and zero). At every time step, all the cells update their states synchronously by applying rules (transition function).

2.3. Chaotic Maps

1D Logistic map is an example chaotic map, it is described as follows:

$$x_{n+1} = u x_n (1 - x_n) \tag{1}$$

Where $u \in [0,4]$, $x_n \in (0,1)$, n=0,1,2,… the research result shows that the system is in a chaotic state under the condition that $3.56994 < u \leq 4$.

The PWLCM can be described in Eq. (4):

$$y_{n+1} = F(y_n, \eta) = \begin{cases} y_n / \eta, & 0 \leq y_n < \eta \\ (y_n - \eta) / (0.5 - \eta), & \eta \leq y_n < 0.5 \\ F(1 - y_n, \eta), & 0.5 \leq y_n < 1 \end{cases} \quad (2)$$

where $y_n \in (0,1)$, n=0,1,2,…, when control parameter $\eta \in (0,0.5)$, Eq. (2) evolves into a chaotic state [20].

3. The Proposed Scheme

3.1. Encryption and Decryption Algorithm

According to Figure 1, the proposed encryption and fingerprinting algorithm can be divided into the following steps:

Step1: Perform two-level DWT decomposition on the original medical image;

Step2: Use logistic map to generate sequences ($x_1 x_2 \cdots x_{M/4 \times N/4}$) respectively, where x_0 and u are given in advance as keys. Then we create a two-dimensional grids of cells G^0, as the seeds of GoL by the sequences, the rule is that if the value of x_i is bigger than the mean value of the sequence, the corresponding cell is alive, else dead. Where G^0 is used to permute the DWT transformed coefficient matrixes;

Step 3: When producing the k th generation G^k by the rules of GoL, the corresponding plain coefficients are put to the scrambling matrix one by one, except the processed;

Step 4: After R rounds iteration, we stop and put the rest of the value into the scrambling image;

Step 5: Fingerprints are embedded into HL and LH sub-spaces using optimization method in [9]. The details about fingerprints embedding will be presented in the next section;

Step 6: Perform two-level IDWT reconstruction with the permutated wavelet transform coefficients. We can get the scrambled and fingerprinted image $I'_{M \times N}$;

Step7: Convert image $I'_{M \times N}$ into a binary matrix $II'_{M \times N}$, and then encode it by DNA coding and transform it into one-dimension nucleotides sequence XI;

Step8: Diffusion processes with DNA addition operation can enhance the resistance to attack. Using the PWLCM map to generate chaotic sequence FP={ $fp_0, fp_1, \ldots, fp_{M \times N}$ }, then we can get the sequence CP={ $cp_0, cp_1, \ldots, cp_{M \times N}$ }, cp_i =ceiling(fp_i) mod 4 to serve as the iteration times, which is one-to-one correspondent with the nucleotide sequence;

Step 9: Compute the base pair of each nucleotide $x_i \in XI$ for cp_i time(s), as show in follows;

For each $x_i \in s_{DNA} \in XI$, do the following increment operation:

$$\begin{cases} x_i = x_i, & cp_i = 0 \\ x_i = A(x_i), & cp_i = 1 \\ x_i = A(A(x_i)), & cp_i = 2 \\ x_i = A(A(A(x_i))), & cp_i = 3 \end{cases}$$

if = 0, do not change x_i;

else if $cp_i = 1$, x_i = A(x_i);

else if $cp_i = 2$, x_i = A(A(x_i));

else if $cp_i = 3$, x_i = A(A(A(x_i))).

where $A(x_i) = x_i + C$, C denotes 01;

Step 10 Convert the sequence XI into a two-dimension matrix, and then convert it into the encrypted image with fingerprint.

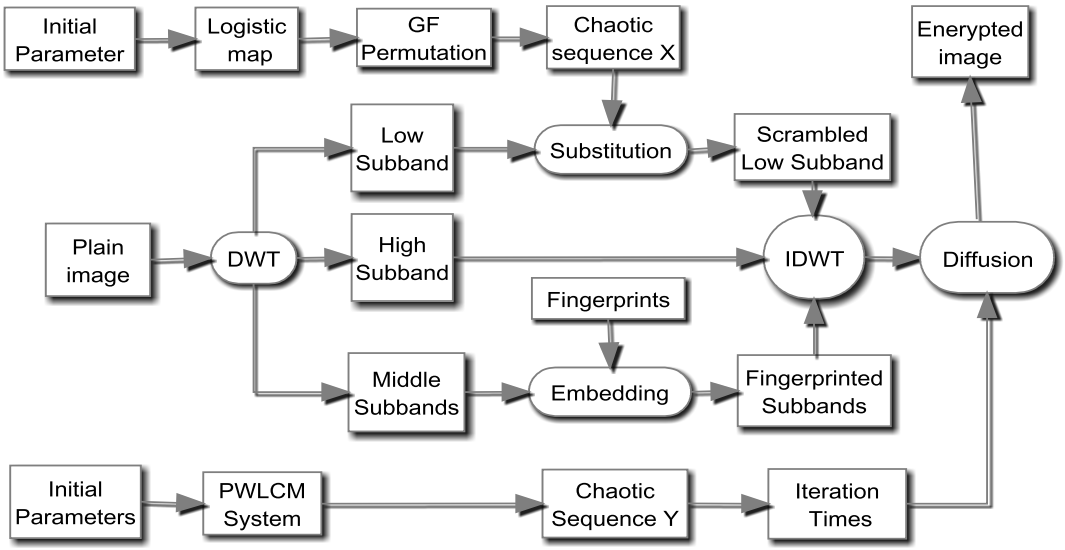


Figure 1. The Architecture of Image Fingerprinting and Encryption Algorithm

3.2. Fingerprints Embedding and Detection

To simplify the description of embedding method, we only discuss how it works on the medical images as well as embedding of a unique fingerprint using an improved QIM scheme [20].We choose the robust coefficients in all LH- level and LH- level subbands to combine a vector, $X_k = (x_1, x_2, ..., x_L)$, as host signals to imbed fingerprint code, where L is the length of codeword, the hiding scheme is as follow:

$$Y_k = Q_\Delta(X_k + W_K + d_k) - W_K - d_k, k = 1, 2, ..., N_u \quad (3)$$

where $Q_\square(\square)$ is the quantization function with step size Δ.

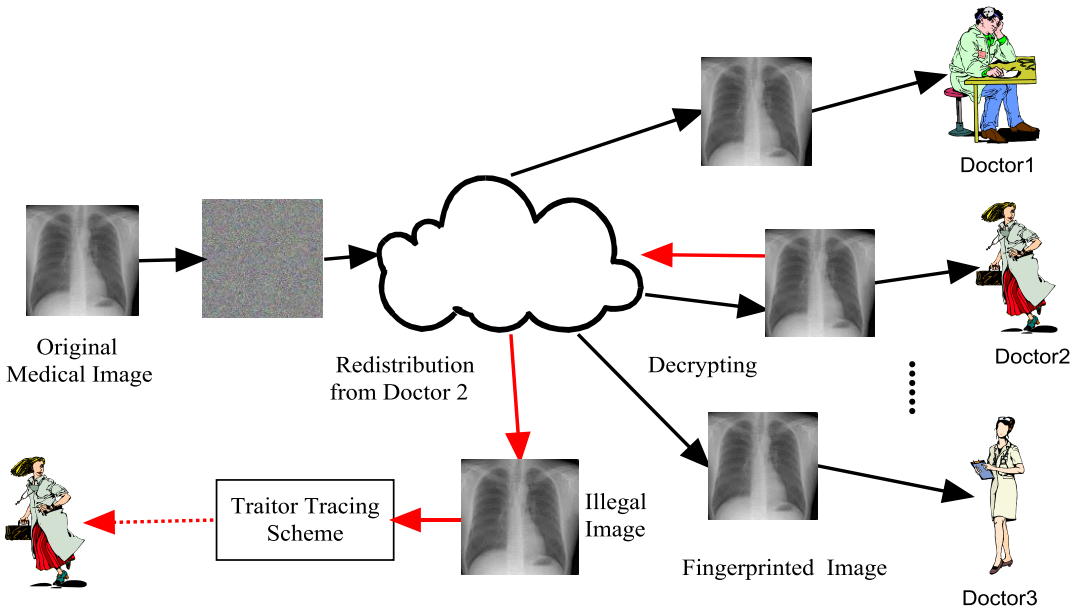


Figure 2. Fingerprinting Scheme for Medical Image Protection

In our implementation, we apply minimum-distance detector from eq. (6) to trace the traitor who leaked information. The L robust coefficients extracted from all LH- level and LH- level subbands, compose a long vector Z with size L. By deducting, the difference is as follow:

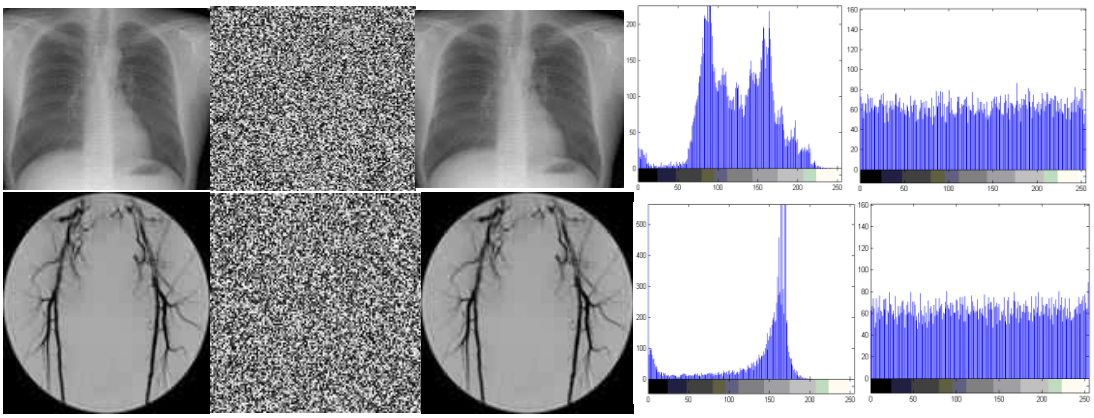
$$\hat{m} = \arg\min_{k=1,2,\ldots N_u} \left\| Z - Y_k \right\|^2 \tag{4}$$

With the above detector, the $\hat{m}$ th user is declared as a traitor.

4. Simulation Results and Security Analysis

In this section, some experimental results are demonstrated to show the effectiveness of the proposed JFE scheme. To demonstrate the security and efficiency of our algorithm, we use some medical images as the original test images, use Matlab 7.8 to simulate the experiment and set parameters x_0 =0. 9432145231, u =3.7425, y_0 = 0.423241243242, η =0.3333.

Figure 3(a) shows the original image, the encrypted image is shown in Figure 3(b). It is obvious that our algorithm achieves good encryption. It is clear that all the encrypted images become noise-like images and are all actually unintelligible. Therefore, the proposed scheme indeed possessed high perceptual security. The fingerprint is embedded in the image during the encryption process. In order to preserve visual quality, the fingerprint in the fingerprinted copy should be imperceptible and perceptually undetectable. Figure 3(c) shows some experimental results of fingerprinted images. It can be observed that the quality of the fingerprinted image doesn't change observably.



(a) (b) (c) (d) (e)

Figure 3. The Experimental Results: (a) the Original Images, (b) the Encrypted Images, (c) the Decrypted Images with Fingerprints, (d) the Grey Histogram of the Original Images, (e) the Grey Histogram of the Encrypted Images

4.1. Ability of Resisting Exhaustive Attack

Our encryption algorithm actually does have some of the following secret keys: (1) Initial values x_0 (Logistic map), y_0 (PWLCM system); (2) Parameters u (Logistic map), η (PWLCM system), k; (3) The iteration times R . The sensitivity to x_0 , y_0 , u and η is considered as 10^{-16} [21], The total key space is about $10^{16\times4}=10^{64}$ .This key space is large enough to resist the brute-force attack. Figure 4(c) is decrypted images with fingerprints by the correct key.

4.2. Resistance to Statistical Attack

Figure 3(d), (e) show the grey-scale histograms of the original image and the encrypted image, respectively. These histograms show that the pixel grey values of the original image are concentrated on some values, but the histogram of the encrypted image is very uniform, which makes statistical attacks difficult.

To test the correlation between two adjacent pixels (horizontally, vertically and diagonally adjacent) in the encryption image, we carry out some simulations. In order to test the correlation of two adjacent pixels, we randomly select 3000 pairs (horizontal, vertical and diagonal) of adjacent pixels from the original image and the encrypted image. Then, calculate their correlation coefficient using the following formulas. Figure 4(a), (b) show the mean correlation of two adjacent pixels in the original medical image and its encrypted image. Figure 4(b) shows that the correlations of adjacent pixels in the encrypted image are greatly reduced. It can clearly be seen that our algorithm can destroy the relativity effectively; the proposed image encryption algorithm has a strong ability to resist statistical attack.

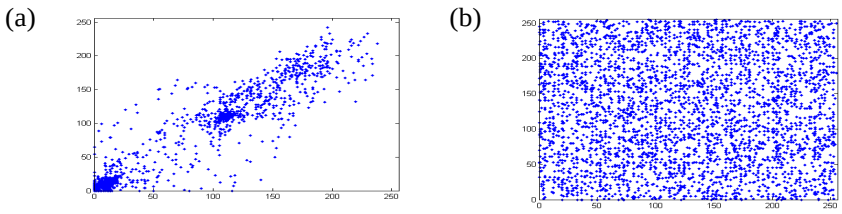


Figure 4. Correlation of Two Horizontally Adjacent Pixels in the Original Image and in the Encrypted Image

4.3. Discussion of the Encryption Process

In Section 3, we knew that the permutation process in Figure 1 only enhances the unintelligibility of the encrypted image. Therefore, even if the chaotic map used in GoL is cracked, the hacker still cannot decrypt the image since the key of diffusion in DNA encryption process remains secret. Figure 5 shows the comparison of when a diffusion process in spatial domain is and is not applied. It is clear that the diffusion process in the proposed scheme can enhance perceptual security. Therefore, if confidentiality is in high demand, the proposed method with diffusion can be applied. Otherwise, the encryption method with only permutation can be performed since only a rough sketch without details would be revealed, making the perceptual quality unacceptable.

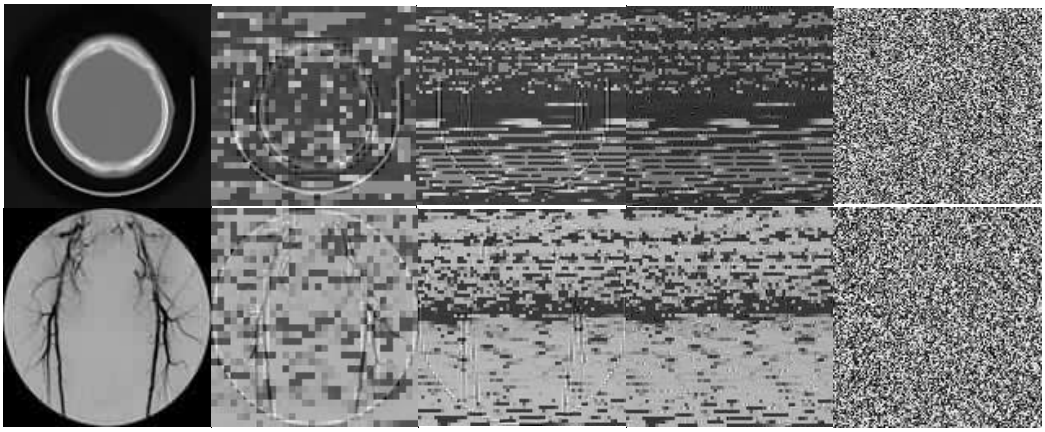


Figure 5. Evaluation of the permutation process; (a) Original medical images, (b) encrypted LL subband of 2-level DWT image via GoL, (c) encrypted LL subband of 1-level DWT image via GoL, (d) encrypted all subbands of 1-level DWT image via GoL respectively, (e) image encryption with permutation on LL subband of 2-level DWT image via GoL and diffusion using DNA computing in spatial domain

4.4. Information Entropy

The information entropy is the most important feature of randomness. If the distribution of grey values is more uniform, the information entropy is greater. The formula for calculating information entropy is defined as follows:

$$H(m) = -\sum_{i=0}^{L} P(m_i) \log_2^{P(m_i)} \quad (5)$$

where $P(m_i)$ is the emergence probability of symbol m_i. We obtained an information entropy H=7.9860, it is can be seen that the proposed algorithm is very effective.

5. Conclusion

The privacy, integrity and confidentiality of medical image are key factors to be considered in the distribution of medical image. In this paper, we proposed a joint fingerprinting and encryption algorithm for medical image security. The fingerprints are embedded into LH and HL subbands of DWT domain. The encryption is based on GoL in DWT domain and DNA sequence addition in spatial domain. This algorithm combines the advantages of the spatial domain and transform domain. The experiment results and algorithm analyses show that the new algorithm possesses a large key space and can resist brute-force, and statistical attacks. Meanwhile, the proposed algorithm is efficient because only the LL coefficient matrix is permutated. Therefore, our algorithm is meant to be a good candidate to ensure the security of medical image distribution.

Acknowledgements

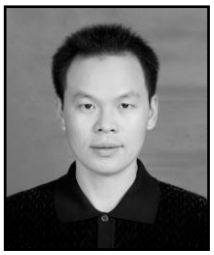
This work is supported by the NSF of China under Grant No. 61370092 and 61370223, Natural Science Foundation of Hubei Province of China (No. 2013CFC005, 2014CFB188), and Youth innovation team project in Hubei Provincial Department of Education (No. T201410).

References

[1] H. Alanazi, H. Jalab, G. Alam, B. Zaidan and A. Zaidan, "Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance", Journal of Medicinal Plants Research, vol. 4, **(2010)**, pp.2059-2074.
[2] S. Das and M. K. Kundu, "Effective management of medical information through ROI-lossless fragile image watermarking technique", Computer Methods and Programs in Biomedicine, vol. 111, **(2013)**, pp. 662-675.
[3] B. Fabian, T. Ermakova and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds", Information Systems.
[4] D. Blumenthal and M. Tavenner, "The "meaningful use" regulation for electronic health records", New England Journal of Medicine, vol. 363, **(2010)**, pp. 501-504.
[5] R. Oppliger, "Security and Privacy in an Online World", Computer, vol. 44, **(2011)**, pp. 21-22.
[6] C. Fu, W.-h. Meng, Y.-f. Zhan, Z.-l. Zhu, F. Lau, C.K. Tse and H.-f. Ma, "An efficient and secure medical image protection scheme based on chaotic maps", Computers in biology and medicine, vol. 43, **(2013)**, pp. 1000-1010.
[7] C. Lee, K. Ho and W. Lee, "A Novel Key Management Solution for Reinforcing Compliance with HIPAA Privacy/Security Regulations", Information Technology in Biomedicine, IEEE Transactions, vol. 15, **(2011)**, pp. 550-556.
[8] R. Norcen, M. Podesser, A. Pommer, H. P. Schmidt and A. Uhl, "Confidential storage and transmission of medical image data", Computers in Biology and Medicine, vol. 33, **(2003)**, pp. 277-292.
[9] P. Fakhari, E. Vahedi and C. Lucas, "Protecting patient privacy from unauthorized release of medical images using a bio-inspired wavelet-based watermarking approach", Digital Signal Processing, vol. 21, **(2011)**, pp. 433-446.
[10] B. Lei, E.-L. Tan, S. Chen, D. Ni, T. Wang and H. Lei, "Reversible watermarking scheme for medical image based on differential evolution", Expert Systems with Applications, vol. 41, **(2014)**, pp. 3178-3188.
[11] M. Arsalan, S.A. Malik and A. Khan, "Intelligent reversible watermarking in integer wavelet domain for medical images", Journal of Systems and Software, vol. 85, **(2012)**, pp. 883-894.
[12] D. Bouslimi, G. Coatrieux and C. Roux, "A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images", Computer Methods and Programs in Biomedicine, vol. 106, **(2011)**, pp. 47-54.
[13] S. Wolfram, M. Gad-el-Hak, A new kind of science, Applied Mechanics Reviews, vol. 56, **(2003)**, pp. B18.

[14] P. Ping, F. Xu and Z.-J. Wang, "Image encryption based on non-affine and balanced cellular automata", Signal Processing, vol. 105, **(2014)**, pp. 419-429.
[15] J. Machicao, A. G. Marco and O. M. Bruno, "Chaotic encryption method based on life-like cellular automata", Expert Systems with Applications, vol. 39, **(2012)**, pp. 12626-12635.
[16] C. Ye, Z. Xiong, Y. Ding, G. Wang, J. Li and K. Zhang, "Joint fingerprinting and encryption in hybrid domains for multimedia sharing in social networks", Journal of Visual Languages & Computing.
[17] R. Enayatifar, A. H. Abdullah and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence", Optics and Lasers in Engineering, vol. 56, **(2014)**, pp. 83-93.
[18] H. Liu, X. Wang and A. kadir, "Image encryption using DNA complementary rule and chaotic maps", Applied Soft Computing, vol. 12, **(2012)**, pp. 1457-1466.
[19] L. M. Adleman, "Molecular computation of solutions to combinatorial problems", Science, vol. 266, **(1994)**, pp. 1021-1024.
[20] G. Cheng, H. Ling, F. Zou and P. Li, "An improved QIM based anti-collusion fingerprinting scheme", IEEE, **(2010)**, pp. 1865-1868.
[21] M. K. Khan, J. Zhang and K. Alghathbar, "Challenge-response-based biometric image scrambling for secure personal identification", Future Generation Computer Systems, vol. 27, **(2011)**, pp. 411-418.

Authors



Conghuan Ye, he received the B.S. and M.S. degree in computer science from Hubei Normal University, Hubei, China, in 2002, and University of Electronic Science and Technology of China, Chengdu, Sichuan, China, in 2005, respectively. Now, his research interests include digital fingerprinting, digital right management, complex network, and cloud computing. Dr. Ye received the scholarship from UESTC from 2003 to 2004.

Dr. Ye, he has co-authored over 30 publications including book chapters, journal and conference papers. He received the Ph.D. degree in computer science and technology, Huazhong University of Science and Technology (HUST) in 2013, Wuhan, Hubei, China. Since 2013, he has been an associate professor with the college of computer science and technology, HBEU.

Zenggang Xiong, he received the the MA degree from Hubei University, China, in 2005, and the PhD degree in computer science from Beijing University of Science and Technology, China, in 2009. He is now a professor in Hubei Engineering University. His research interests are in the areas of peer-to-peer computing, Cloud computing, distributed systems and big data.

Yaoming Ding received the the MA degree from Huazhong Normal University, China, in 2000, and the PhD degree in education from Huazhong Normal University, China, in 2011. He is now a professor in Hubei Engineering University. His research interests are in the areas of optical communication technology and cloud computing.

Xuemin Zhang, she received the the Bachelor degree in computer science from Hubei Normal University, China, in 2001, and the MA degree in computer science from Wuhan University of Technology, China, in 2009. She is now an associate professor in Hubei Engineering University. Her research interests are in the areas of Cloud computing, distributed systems, Service Computing. She is a member of the IEEE and the ACM.

Guangwei Wang, he received the B.S. and M.S. degree in computer science from Huazhong Normal University, Wuhan, China, in 2005 and 2008, respectively. He received the Ph.D. degree from Huazhong University of Science and Technology in 2012. Now, He works in School of Computer and Information Science, Hubei Engineering University and his research interests include Computer vision and video analysis. He has co-authored more than 10 papers published in various journals.

Fang Xu, he received the B.S. and M.S. degree in computer science from Hubei Engineering University, Hubei, China, in 2003, and Wuhan University, Wuhan, Hubei, China, in 2009, respectively. Now, his research interests include Mobile Social Networks, digital fingerprinting, Machine Learning, and cloud computing. He has co-authored over 20 publications including journal and conference papers. He is currently a Ph.D. student in the Wuhan University at Wuhan, majoring in computer science and technology.