Journal of Zhejiang University SCIENCE A
ISSN 1673-565X (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

Bluetooth-based authentication system for ambient intelligence*

Jian HE†1, Hui LI2, Yong ZHANG3, Zhang-qin HUANG1

([1]School of Software Engineering, Beijing University of Technology, Beijing 100022, China)

([2]College of Computer Science, Beijing University of Technology, Beijing 100022, China)

([3]College of Electronic Information and Automation, Tianjin University of Science and Technology, Tianjin 300222, China)

†E-mail: Jianhee@bjut.edu.cn

Received Sept. 25, 2007; revision accepted Jan. 16, 2008; published online Apr. 17, 2008

Abstract: According to the requirement of natural human-computer interaction for Ambient Intelligence (AmI), a Bluetooth-based authentication technique is provided. An authentication network combining advantages of Bluetooth ad hoc network with the Ethernet is introduced first in detail. Then we propose a Bluetooth badge for storing the user's identification information. Finally, the authentication system based on Bluetooth badge and authentication network is introduced. It is demonstrated experimentally that the Bluetooth-based authentication technique can authenticate the user automatically.

Key words: Bluetooth, Ambient Intelligence (AmI), Authentication
doi:10.1631/jzus.A071516 **Document code:** A **CLC number:** TP311

INTRODUCTION

The concept of Ambient Intelligence (AmI) is presented by the Information Society Technology Advisory Group (ISTAG). It describes a vision of the information society where the emphasis is on greater user friendliness, more efficient services support, user-empowerment, and support for human interactions (Ducatel *et al*., 2000). Under this circumstance, people are surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects and in an environment that is capable of recognizing and responding to the presence of different individuals in a seamless, unobtrusive and often invisible way (Weber, 2003). Development of embedded technology and human-computer interaction technology is improving the realization of this vision continuously.

The most important goal of AmI is to provide personalized services according to the individual's living habits (Hagras *et al*., 2004). Moreover, identifying a user uniquely is the precondition of offering personalized services for individuals. Hence, identity authentication is a key factor for AmI. Conventionally, the process of identity authentication requires the user to interact with the authentication system consciously. However, it is unfit for the natural interaction which is required by the AmI (Naqvi and Riguidel, 2004). When the problem is concerned, we introduce a Bluetooth-based authentication system, in which the authentication procedure is accomplished automatically by an electronic device carried by the user, and the user is not aware of the authentication procedure.

TECHNOLOGY FOUNDATION

Being one of the wireless standards, Bluetooth operates at 2.4 GHz in the globally available ISM band, and is devoted to short range (<10 m for Class 2 devices), low data-rate (<1 Mbits/s) communication. Bluetooth modules dissipate less power, are smaller and less expensive than IEEE802.11b ones (Han *et al*., 2004), and can be easily integrated into the embedded system. Therefore, Bluetooth technology has been chosen as the best wireless standard solution for sensor networking.

* Project supported by the National Natural Science Foundation of China (No. 60773186), and the Science and Technology Research Foundation of the Beijing Municipal Education Commission of China (No. KM200710005018)

For the above reasons, we use a Bluetooth badge (namely Blue Badge) to store the user's identification information. In the AmI environment, a Blue Badge adorned by the user automatically accomplishes the authentication through the Bluetooth network (Ding, 2005).

Network architecture

The system architecture which has been designed as simple as possible takes the advantages of the Bluetooth ad hoc network (Bray and Sturman, 2002) and the Ethernet. Bluetooth offers a simple master-slave network topology, called Piconet, where a master can control up to seven slaves; network nodes can be dynamically connected and disconnected from the Piconet at any time and this operation is transparent to end users. Fig.1 shows the proposed system.

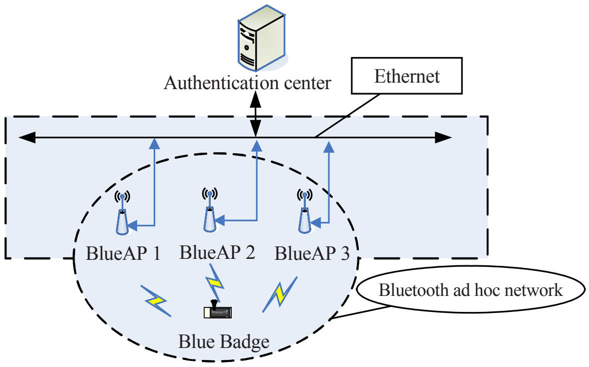


Fig.1 Network topology of the authentication system for Ambient Intelligence (AmI)

(1) Blue Badge. Being a slave mode device, a Blue Badge stores the user's identification information which is unique, and can identify the user exclusively. When a user with a Blue Badge comes into the AmI environment, the Blue Badge connects to the authentication center through the Bluetooth ad hoc network, and the individual identification is submitted to the authentication center.

(2) BlueAP. As a master mode device, BlueAP connects to the Blue Badge and the Ethernet. When a user with a Blue Badge comes into the AmI environment, the BlueAP gets the user ID from the Blue Badge, and submits it to the authentication center through the Ethernet.

(3) Authentication center. It authenticates the user ID provided by the BlueAP through the Ethernet, and authorizes the user privilege.

In this system, Blue Badge is a small and portable embedded equipment with limitations in computation, communication and battery life. Being a component of the Bluetooth ad hoc network, the BlueAP is flexible when the Bluetooth network is being deployed, but it will be in a fixed position as soon as the network is deployed completely. Compared with the Blue Badge, the BlueAP can do more complex computing as it has less limitation in physical size and power. In the authentication system, the authentication center has the most powerful computing ability. Due to the Ethernet connection, communication between the BlueAP and the authentication center is very fast. During the implementation of the authentication system, the majority of computation and communication is carried out in the authentication center, which reduces the computation on the Blue Badge. As a result, the authentication efficiency is enhanced.

Blue Badge construction

Different authentication techniques have different features and, hence, are fit for different situations. For example, the authentication system based on secret information has the disadvantage of leaking the password, but it is widely used in the mainstream computer system because of its low cost and easy realization. The authentication system based on token requires the user to carry a hardware device, which is burdensome for the user and costs more. However, it is widely used in the area of finance and safety guarantee because of its high security (Li *et al*., 1999). The authentication system based on biologic features reduces the risk of losing the keepsake and can provide higher security, but it costs even more (Li and Ou, 2000). Therefore, the selection of an appropriate authentication technique for an application needs to balance the security, computation speed and cost.

The Blue Badge has limitation in computation and battery life, however, both the keepsake and the biologic feature require powerful computing ability. Therefore, the DES (data encryption standard) encryption and the challenge/response technology are combined to realize the authentication system for the AmI.

As an embedded Bluetooth device, the Blue Badge is composed of a basic Bluetooth communication module and a memory which stores the user ID and the shared key. The Bluetooth communication module uses a BlueCore chip produced by CSR Company (CSR, 2006), and its main functions include initialization and communication with the BlueAP. The user ID composed of eight ASCII characters identifies the user uniquely. Every 128-bit shared key corresponds to a unique user ID, so different users hold different shared keys. Besides, the authentication center preserves all of the shared keys and forms an indexing table which stores the above correlation between the user ID and the shared key.

AUTHENTICATION PROTOCOL

The topological feature of the authentication system for AmI leads to the following two steps: (1) authentication between the Blue Badge and the BlueAP; (2) authentication between the BlueAP and the authentication center. In the followings, we will introduce these two steps in detail.

Authentication between Blue Badge and BlueAP

First, the Blue Badge communicates with the BlueAP through the Bluetooth Piconet. Since the Bluetooth technology itself includes perfect authentication, authorization and encryption mechanisms (Chatschik, 2001), we take advantage of these mechanisms to implement the authentication between the Blue Badge and the BlueAP (Gui and Zhang, 2002).

Fig.2 shows that the Blue Badge sends a RADIUS Access-Request message to the BlueAP, and the BlueAP returns an Access-Challenge message that carries a random sequence encrypted by its shared key, and then the Blue Badge responds to it by encrypting the random sequence with the shared key. At last, the BlueAP finishes the authentication by comparing the response result with the encrypted random sequence. The key authentication procedure is as follows:

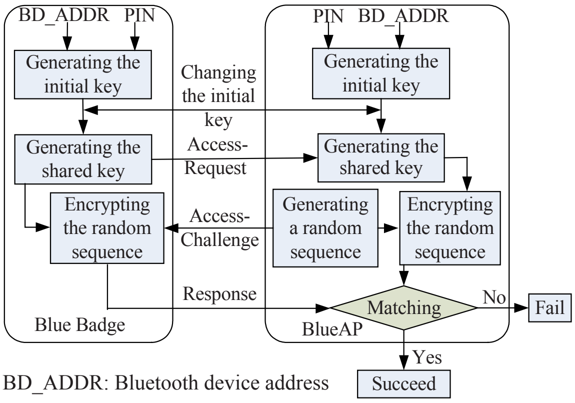

BD_ADDR
PIN
Generating the initial key
Changing the initial key
PIN
BD_ADDR
Generating the initial key
Generating the shared key
Access-Request
Generating the shared key
Encrypting the random sequence
Access-Challenge
Generating a random sequence
Encrypting the random sequence
Response
Matching
No
Fail
Blue Badge
BlueAP
Yes
Succeed
BD_ADDR: Bluetooth device address

Fig.2 Authentication between Blue Badge and BlueAP

1. Pairing. The Bluetooth device creates an initial key using the PIN code and the Bluetooth device address (namely BD_ADDR) (Wang, 2003). The PIN code is an exclusive parameter set by the system, and the rest of the parameters (such as the authentication key and the encryption key) have close relationship with the PIN code. BD_ADDR is a unique IEEE address assigned to every Bluetooth device by the producer. During the authentication procedure, the BlueAP obtains the Blue Badge's BD_ADDR through the Bluetooth inquiring procedure. In fact, the authentication between the Blue Badge and the BlueAP is a procedure of matching the PIN code. So the PIN code is the key parameter for the authentication.

2. Generating the shared key. The shared key, namely the link key, is a half perpetual key. During the implementation, we select the associated key which has higher security as the shared key.

3. Realizing the Challenge-Response authentication. The authentication between the Blue Badge and the BlueAP, on balance, implements the first authentication step if the PIN codes are matched, and the following encryption procedure will be stopped if the PIN codes do not match. The encryption key which will be used by the next encryption procedure is also generated if the first authentication step is passed. After that, a safe channel between the Blue Badge and the BlueAP is built through the encryption key to transmit data. The key steps to build the safe channel are as follows:

(1) Consulting the encryption parameters, including the encryption pattern and the length of the encryption key.

(2) Generating the encryption key from the current link key, a 96-bit ciphering offset number (COF) and a 128-bit random number. The COF is based on the authenticated ciphering offset (ACO), which is generated during the authentication process (Wang, 2003).

(3) Encrypting the payloads of the packets.

During the authentication, the group messages encrypted by using the initialization key (or the shared key) are transmitted through the Bluetooth link. The possibility of deducing the PIN code conversely is very low, even though the attacker has obtained the group messages by monitoring the Bluetooth channel. So the PIN code is safe enough as long as they are safely stored in the Blue Badge. In addition, the authentication between the Blue Badge and the BlueAP does not change the user information, which is transmitted through the safe channel. Thus the security of the user information can be guaranteed.

Authentication between BlueAP and authentication center

The BlueAP communicates with the authentication center through the Ethernet, so conventional authentication protocols can be applied to implement the authentication. For example, the Kerberos protocol can be adopted to increase the reliability of the system. However, using the complicated authentication protocol between the BlueAP and the authentication center cannot improve the security, so we adopt the Challenge-Response protocol based on a symmetric key. Fig.3 shows the authentication protocol. The authentication between the BlueAP and the authentication center will be implemented only after the first authentication step has been finished and the Blue Badge has sent the user information to the BlueAP successfully.

After getting the user information from the Blue Badge through the encryption channel, the BlueAP selects the user ID and sends it to the authentication center. The authentication center checks the user information table according to the user ID, and gets the user's shared key. And then, the authentication center generates a random sequence and sends it back to the BlueAP (namely Challenge). Meanwhile, the authentication center encrypts the random sequence using the shared key. After receiving the random sequence, the BlueAP encrypts it using the shared key and sends it back to the authentication center (namely Response). The authentication center implements the authentication by matching the random sequence.

We can know from Fig.3 that the authentication center includes two key modules:

(1) The algorithm for generating a random sequence. A random sequence is used by the authentication center to initiate the Challenge, and it must be unrepeatable and uncertain. So the linear congruential generator was selected to generate the random sequence.

(2) The encryption algorithm. We use the DES algorithm to encrypt the random sequence.

APPLICATION

During the implementation of AmI and the embedded system which is supported by the "211 Project" of Beijing University of Technology (Zhang *et al*., 2006), we applied the Bluetooth-based authentication technique to build an AmI-Space. Fig.4 shows the AmI-Space architecture.

Architecture of AmI-Space

In AmI-Space, there are different kinds of electric appliances (such as TV, fridge, microwave oven, projector, etc.), which are distributed in different areas in invisibly computing form and can provide a user with services automatically. As soon as the user with a Blue Badge enters the AmI-Space, the authentication system for AmI will automatically authenti-

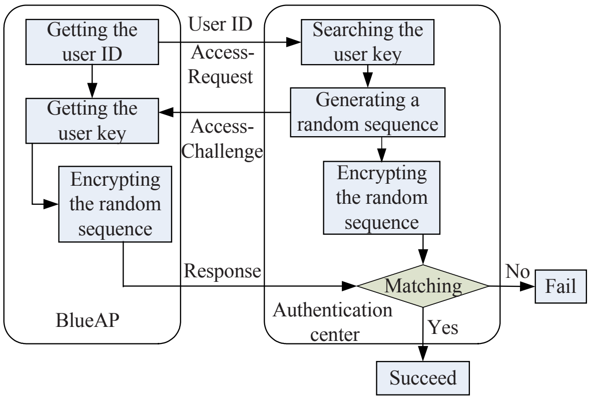


Fig.3 Authentication protocol between the BlueAP and the authentication center

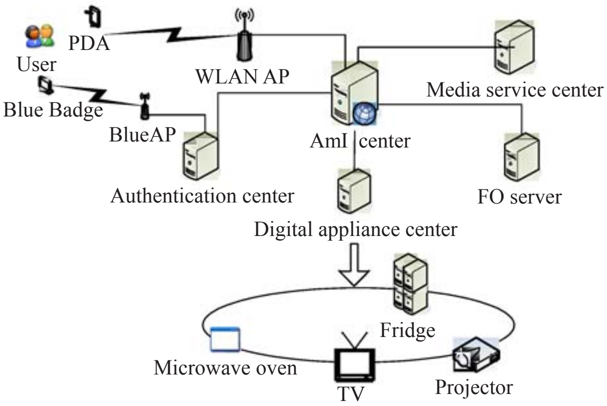


Fig.4 Architecture of the AmI-Space

cate the user. In the next step, the AmI center searches the user database, and obtains the user privilege and the personal video/audio service data. Then, the AmI center pushes the personal information to the user's PDA through WLAN. After the user has selected the service items through the PDA, the facial orientation (FO) recognition system verifies the user's face orientation, and instructs the projector to projects the service contents to the wall facing the user. At last, on the user's departure from the environment, the authentication system for AmI will sense this event, stop the service and log the user out.

Fig.5 is a scene for the AmI-Space, showing that the projector automatically projects the service contents to the wall facing the user according to the individual face orientation (Chen and Li, 2005).

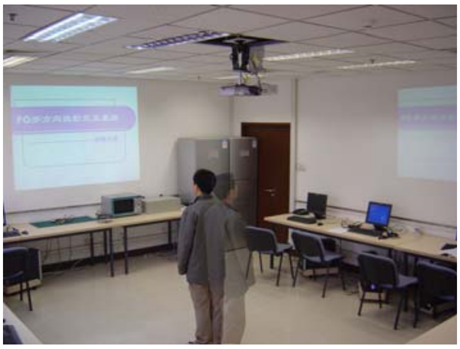


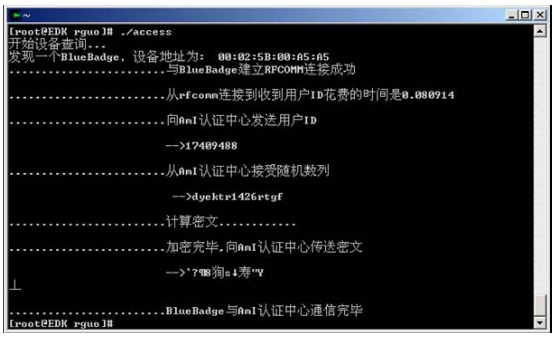
Fig.5 A scene of the facial orientation recognition system in the AmI-Space

Example of authentication

Though there are other wireless applications in the AmI-Space, for example, WLAN and infrared controller, the user with a Blue Badge will be authenticated by the authentication center in 1 s after he/she comes into the AmI-Space. It proves that the Bluetooth-based authentication system is robust.

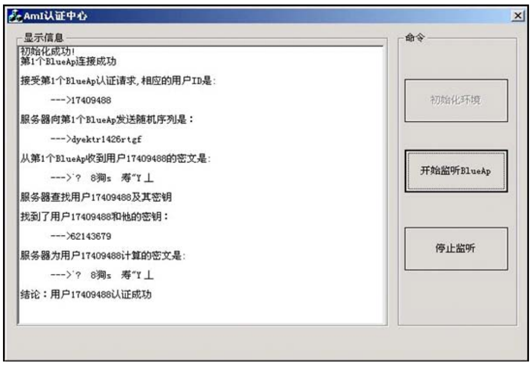
Fig.6 shows a BlueAP instance in the AmI-Space. When a user with a Blue Badge comes into the environment, the BlueAP discovers the device and creates a safe channel. Then, the BlueAP gains the user ID and interacts with the authentication center to carry out the authentication in sequence.

Fig.7 is an authentication center instance corresponding to Fig.6. It shows that the BlueAP interacts with the authentication center to implement the user authentication.



```
[root@EDK rguo]# ./access
开始设备查询...
发现一个BlueBadge, 设备地址为:  00:02:5B:00:A5:A5
.........................与BlueBadge建立RFCOMM连接成功

.........................从rfcomm连接到收到用户ID花费的时间是0.080914

.........................向AmI认证中心发送用户ID

                         -->17409488

.........................从AmI认证中心接受随机数列

                          -->dyektr1426rtgf

.........................计算密文............

.........................加密完毕,向AmI认证中心传送密文

                         -->`?¶8狗s↓寿"Y
⊥

.........................BlueBadge与AmI认证中心通信完毕
[root@EDK rguo]#
```

Fig.6 An example for BlueAP in the AmI-Space (in Chinese)



```
初始化成功!
第1个BlueAp连接成功

接受第1个BlueAp认证请求,相应的用户ID是:

      --->17409488

服务器向第1个BlueAp发送随机序列是:

      --->dyektr1426rtgf

从第1个BlueAp收到用户17409488的密文是:

      --->`?  8狗s  寿"Y⊥

服务器查找用户17409488及其密钥

找到了用户17409488和他的密钥:

      --->62143679

服务器为用户17409488计算的密文是:

      --->`?  8狗s  寿"Y⊥

结论:用户17409488认证成功
```

Fig.7 An example for the authentication center (in Chinese)

Response delay and power consumption

The Bluetooth standard is a complex standard with many degrees of freedom that the designer can use at the application layer to reduce the power dissipation, e.g., the choice of different modes in which each slave can operate (active, sniff, etc.). In order to select a reasonable mode for the Blue Badge which both saves power and reduces the response delay, many tests have been carried out to obtain the Blue Badge's different response delay and power consumption.

Table 1 shows the Blue Badge's different response delay and its corresponding power consumption in four modes. In addition, we test the Blue Badge's response delay 10 times for each mode. Fig.8 shows the trendline of the response delay for each mode. We can draw a conclusion from Table 1 and Fig.8 that the more the sniff slots, the more the response delay and the less the power consumption. We can see that Mode 2 is the most fit for the Blue Badge for a trade-off between the response delay and the power consumption.

Table 1 Response delay and power consumption for four modes

Mode	Sniff slots*	Sniff attempt slots*	Sniff timeout slots*	Max response delay (ms)	Average response delay (ms)	Average power consumption (mA)
1 (Active)	–	–	–	198	156	35.65
2 (Sniff)	500	15	3	500	381	6.09
3 (Sniff)	1600	15	3	1687	1608	5.22
4 (Sniff)	3000	15	3	2828	2480	4.78

* A slot=0.6 ms

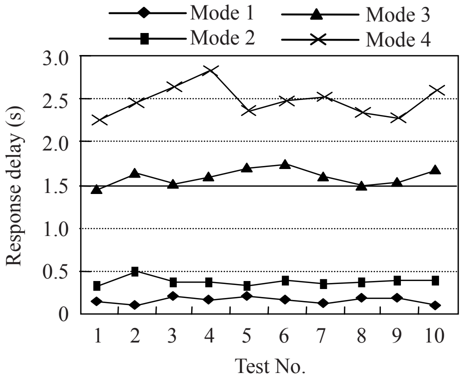


Fig.8 Trendline of the response delay for each mode

Due to the good trade-off between the response delay and the power consumption, Mode 2 is selected as the Blue Badge's mode of operation. It proves experimentally that the life of a lithium battery (3.7 V, 320 mA) is over 12 h in the AmI-Space in Mode 2.

CONCLUSION

It has been proved by the authentication system for Ambient Intelligence that the Bluetooth-based authentication technique reduces the human-computer interaction compared to the conventional identity authentication and implements a natural interaction mode which is more close to the natural human-human interaction mode. Now, our system has been successfully applied in the Ambient Intelligence and embedded system supported by the "211 Project" of Beijing University of Technology.

References

Bray, J., Sturman, C.F., 2002. Bluetooth: Connect without Cables (2nd Ed.). Prentice Hall PTR, Upper Saddle River, New Jersey.

Chatschik, B., 2001. An overview of the Bluetooth wireless technology. *IEEE Commun. Mag.*, **39**(12):86-94. [doi:10.1109/35.968817]

Chen, R., Li, H., 2005. Facial Orientation Analysis and Application in Human-Computer Interactive System—Convergence of Computing Technologies in the New Era. Proc. 8th Int. Conf. for Young Computer Scientists. Beijing, p.553-560.

CSR (Cambridge Silicon Radio Ltd.), 2006. BlueCore2-External Product Data Book. Http://www.csrsupport.com/CSR/Data Sheets/BlueCore2-External Data Sheet/262_Blue Core2-External Data Book.pdf

Ding, Z.B., 2005. Research and Implementation of Bluetooth Based Authentication System in Ambient Intelligent. MS Thesis, Xi'an Jiaotong University, Xi'an, China (in Chinese).

Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J., Burgelman, J.C., 2000. Scenarios for Ambient Intelligence in 2010. Http://www.philips.co.kr/Assets/Downloadablefile/eur19763en-1505.pdf

Gui, J.H., Zhang, H.S., 2002. Security resolution of Bluetooth. *Computer Appl.*, **22**(10):12-17 (in Chinese).

Hagras, H., Callaghan, V., Colley, M., Clarke, G., Pounds-Cornish, A., Duman, H., 2004. Creating an ambient-intelligence environment using embedded agents. *IEEE Intell. Syst.*, **19**(6):12-20. [doi:10.1109/MIS.2004.61]

Han, J.H., Duan, L.L., Zhang, J.J., Wang, J.H., 2004. Development of Bluetooth subsystem of embedded information appliance system. *J. Syst. Simul.*, **16**(12):2825-2827 (in Chinese).

Li, T., Ou, Z.Y., 2000. Development and application of individual feature based authentication technique. *Computer Eng.*, **26**(12):69-70 (in Chinese).

Li, Z.X., Zhan, B.H., Yang, Y.X., 1999. Development of authentication theory and technique. *Chin. J. Electr.*, **27**(1):98-102 (in Chinese).

Naqvi, S., Riguidel, M., 2004. Security Architecture for Heterogeneous Distributed Computing Systems. Proc. 38th Annual Int. Carnahan Conf. on Security Technology, p.34-41. [doi:10.1109/CCST.2004.1405366]

Wang, C.L., 2003. Study on Bluetooth security. *J. Shandong Univ. Sci. Technol. (Nat. Sci.)*, **22**(4):61-64 (in Chinese).

Weber, W., 2003. Ambient Intelligence—Industrial Research on a Visionary Concept. Proc. Int. Symp. on Low Power Electronics and Design, p.247-251.

Zhang, Y., Hou, Y.B., Huang, Z.Q., Li, H., Chen, R., 2006. A Context-Aware AmI System Based on MAS Model. Intelligent Int. Conf. on Intelligent Information Hiding and Multimedia, p.703-706. [doi:10.1109/IIH-MSP.2006.265098]