Information Technology Journal 7 (1): 63-69, 2008
ISSN 1812-5638

A New Data Encryption Algorithm Based on the Location of Mobile Users

Hsien-Chou Liao and Yun-Hsiang Chao
Department of Computer Science and Information Engineering, Chaoyang University of Technology,
168 Jifong E. Rd., Wufeng Township Taichung County, 41349, Taiwan (R.O.C.)

Abstract: The wide spread of WLAN and the popularity of mobile devices increases the frequency of data transmission among mobile users. However, most of the data encryption technology is location-independent. An encrypted data can be decrypted anywhere. The encryption technology cannot restrict the location of data decryption. In order to meet the demand of mobile users in the future, a location-dependent approach, called location-dependent data encryption algorithm (LDEA), is proposed in this paper. A target latitude/longitude coordinate is determined firstly. The coordinate is incorporated with a random key for data encryption. The receiver can only decrypt the ciphertext when the coordinate acquired from GPS receiver is matched with the target coordinate. However, current GPS receiver is inaccuracy and inconsistent. The location of a mobile user is difficult to exactly match with the target coordinate. A toleration distance (TD) is also designed in LDEA to increase its practicality. The security analysis shows that the probability to break LDEA is almost impossible since the length of the random key is adjustable. A prototype is also implemented for experimental study. The results show that the ciphertext can only be decrypted under the restriction of TD. It illustrates that LDEA is effective and practical for data transmission in mobile environment.

Key Words: data encryption, GPS, mobile computing, location-based service

INTRODUCTION

Since the removal of signal-degrading Selective Availability (SA) from GPS (Global-Positioning System) signals on the 1st May 2000, it is now possible to use hand-held GPS to navigate to within a few meters. The differential GPS (DPGS) can even provide the accuracy to less than one meter. Now, GPS receiver is popular used in our daily life, such as car navigation, fleet management, and so on. In the past, GPS receiver is connected to the mobile devices, such as PDA (personal digital assistant), via cable or Bluetooth. It is a little inconvenient for users. Therefore, a PDA with an integral GPS receiver, called GPS PDA, is designed and announced on the mid of 2005. GPS PDA is also equipped with most of the wireless communication capabilities, including GSM/GPRS/EDGE, quad-band GSM phone capabilities, IEEE 802.11g, etc. The size and weight of GPS PDA is close to the mobile phone. But, it's computing power and programming interface is better than mobile phones. It is expectable that the mobile phones will be replaced by such kind of PDA in the future. Unlike the mobile phones which data transmission is mostly based on SMS (Short Message Service), the types and quantities of data transmitted among GPS PDAs must be diverse and huge just like desktop PCs. That is, the data transmission among mobile devices will become more and more frequent according to the above trend.

On the other hand, many methods are proposed for the security of data transmission; for example, M. Aikawa et al. proposed a light-weight encryption algorithm for the copyright protection (Aikawa et al., 1998). T. Jamil proposed an enhanced algorithm for the typical DES algorithm, called AES (Jamil, 2004). J. Jiang proposed a parallel processing algorithm for the RSA (Jiang, 1996). S. Lian et al. proposed a fast video encryption scheme based on chaos (Lian et al., 2004). M. McLoone and J. V. McCanny designed a hardware circuit for DES based on the FPGA technique (McLoone and McCanny, 2000). M. Shaar et al. proposed a new data encryption algorithm, called HHEA (Shaar et al., 2003). M. E. Smid and D. K. Branstad analyzed the past and future of DES algorithm (Smid and Branstad, 1988). Y. P. Zhang et al. proposed a stream cipher algorithm with respect to the traditional block-based cipher approaches (Zhang et al., 2004).

However, these methods are location-independent. The sender cannot restrict the location of the receiver for data decryption. If the data encryption algorithm can provide such function, it is useful for increasing the security of mobile data transmission in the future. Therefore, a location-dependent data encryption algorithm (LDEA) is proposed in this paper. The latitude/longitude coordinate is used as the key for data encryption in

Corresponding Author: Hsien-Chou Liao, Department of Computer Science and Information Engineering,
Chaoyang University of Technology, 168 Jifong E. Rd., Wufeng Township Taichung County, 41349,
Taiwan, ROC Tel: +886-4-23323000/4211 Fax: +886-4-23742375

LDEA. When a target coordinate is determined for data encryption, the ciphertext can only be decrypted at the expected location. Since the GPS receiver is inaccurate and inconsistent depending on how many satellite signals received. It is difficult for receiver to decrypt the ciphertext at the same location exactly matched with the target coordinate. It is impractical by using the inaccurate GPS coordinate as key for data encryption. Consequently, a toleration distance (TD) is designed in LDEA. The sender can also determine the TD and the receiver can decrypt the ciphertext within the range of TD. In order to verify the performance of LDEA, a prototype tool is also implemented and tested in an outdoor experimental site. The experimental result illustrates that LDEA is effective and practical for data transmission in mobile environment.

RELATED WORKS

The popular of indoor or outdoor positioning devices cause the location-based service (LBS) is getting important. LBS is a service depending on a certain location. Systems can provide LBSs according to the location of users. For example, a user may query "where is the nearest restaurant?". Current LBSs can be classified into four categories: emergency service, information service, tracking service, and entertainment service (Mohapatra and Suma, 2005). Emergency services include safety alarm, public safety, and so on. For example, Y. Zhang et al. proposed location-based keys for the sensor network (Zhang et al., 2005). It was an authentication scheme between sensor nodes. Information services include the news, sport, weather, shopping, yellow page, and so on (Becker and Durr, 2005)(Toye and Sharp, 2005). Tracking services include the property, military, cargo tracking, and so on. M. Gruteser and X. Liu discussed the privacy protection problems related to the tracking service (Gruteser and Liu, 2004). A disclosure-control algorithm was proposed to hide users' position in sensitive area. Entertainment services include dating, game playing, and so on. N. Eagle and A. Pentland designed a Bluetooth access point, called BlueDar (Eagle and Pentland, 2005). It can interchange information with the mobile devices of the passing passengers. If the passenger predefines the demands of friends, such as age, hobby, BlueDar can match his demands with the collected information of the passengers. J. Xu et al. proposed a D-tree structure for the query planning of LBSs (Xu et al., 2004). The above researches mainly focus on the promotion of LBSs but not on the data security in the mobile environment.

Several location-dependent data encryption methods were proposed. T. Mundt proposed a location-dependent digital rights management system (Mundt, 2005). Location is essential for controlling access to resources protected by the digital rights. A trusted device which incorporates a precise secure clock and a GPS receiver is implemented. The encrypted digital material can be decrypted when the device is in a specified area.

D. Qiu *et al* at Stanford University proposed an authentication protocol using Loran signal (Qiu et al., 2006). Loran is a low frequency pulsed navigation system. It can be made resistant to unauthorized used and tampering. Therefore, a signal authentication protocol, called TESLA, is proposed and implemented. The result shows that TESLA provides strong protection against location spoofing.

H. C. Liao et al. proposed a location-dependent data encryption approach for mobile information system (Liao et al., 2007). The approach is based on a reverse hashing principle. A series of session keys is generated based one-way hash function. They are generated for mobile client and server in a secure network simultaneously. When the mobile client is operated in an insecure network of the outdoor environment, the session key is incorporated with the GPS coordinate for ensuring the data is decrypted at the desired location.

Besides, L. Scott and D. E. Denning proposed a data encryption algorithm by using the GPS, called Geo-Encryption (Scott and Denning, 2003). Geo-Encryption was based on the traditional encryption system and communication protocol. For the sender, the data was encrypted according to the expected PVT (position, velocity, and time) of the receiver. A PVT-to-GeoLock mapping function was used to get the GeoLock key. GeoLock key was performed bitwise exclusive-OR with a generated random key to get a GeoLock session key. This session key was then transmitted to the receiver by using asymmetric encryption. For the receiver, an anti-proof GPS receiver was used to acquire the PVT data. Then, the same PVT-to-GeoLock mapping function was used to get the GeoLock key. The key was performing exclusive-OR operation with the received GeoLock session key to get the final session key. The final session key was used to decrypt the ciphertext. However, the PVT-to-GeoLock mapping function is the primary mechanism to ensure that the data can be decrypted successfully. It is troublesome for sender and receiver to own the same mapping function before the data transmission if they communicate occasionally. The design of LDEA can improve the above problem by skipping such mapping function.

MATERIALS AND METHOD

The purpose of LDEA is mainly to include the latitude/longitude coordinate in the data encryption and thus to restrict the location of data decryption. A

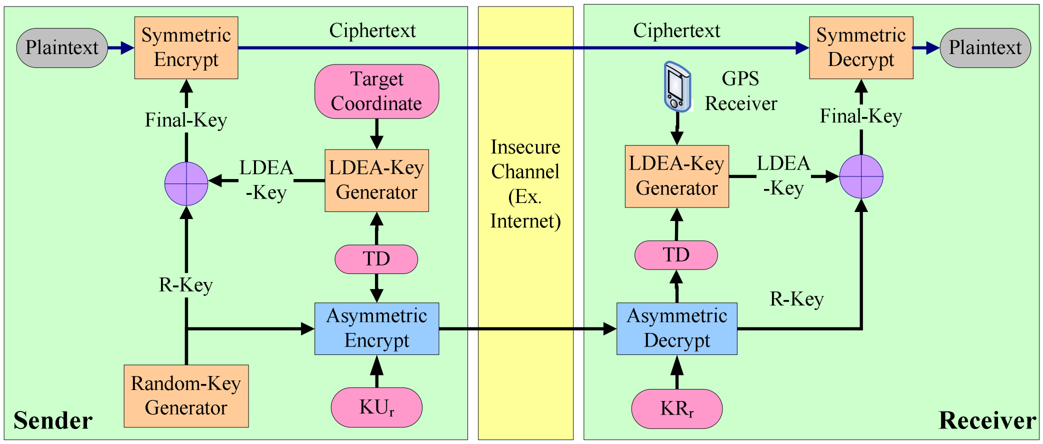


Fig.1: The LDEA process

toleration distance (TD) is designed to overcome the inaccuracy and inconsistent problem of GPS receiver. The process of LDEA is shown in Figure 1. When the target coordinate and TD (toleration distance) is given by the sender on the left-hand side, an LDEA-key is generated from latitude/longitude coordinate and TD. The random-key generator issues a session key, called R-key. Then, the final-key for encrypting the plaintext is generated by exclusive-or R-key with LDEA-key. The final-key can be used for the symmetric encrypt algorithm, such as DES, AES, triple-DES, etc. In the bottom of Figure 1, KUr and KRr is the public and private keys generated on the receiver side. KUr is transmitted to the sender side firstly. Then, TD and R-key is transmitted via asymmetric encryption algorithm. When the receiver gets the TD and R-key, the LDEA-key can be generated from TD and the coordinate acquired from GPS receiver. The final-key can be generated by exclusive-or R-key with LDEA-key. If the acquired coordinate is matched with the target coordinate within the range of TD, the ciphertext can be decrypted back to the original plaintext. Otherwise, the result is indiscriminate and meaningless.

The target coordinate can be determined by the sender or receiver. If it is determined by the sender, the sender can inform the receiver the physical location for data encryption. A secure communication, such as telephone, is convenient and safety for the sender to notify the receiver. If the target coordinate is determined by the receiver, the receiver can inform the sender in the same way, e.g., telephone. After the sender gets the target coordinate, the data can be transmitted to the receiver according to the above process.

The generation of LDEA-key, R-key, and final-key is presented in more details. An example shown in Figure 2 is used to illustrate the generation process. TD is assumed as five meters in the example.

- **Transform latitude/longitude coordinate:** The format of coordinate acquired from the GPS receiver is WGS84 (world geodetic system 1984) defined in NMEA (National Marine Electronics Association) specification. For example, “E 12134.5971” means 121 degrees and 34.5971 minutes east longitude. “N 2504.7314” means 25 degrees and 4.7314 minutes north latitude. The coordinates are multiplied 10000 to be an integer. Then, the integer is divided by a value corresponding to the TD in order to allow the coordinate inaccuracy. According to the estimation of CoordTrans tool of Franson Company, the values are 5.4 and 6 for latitude and longitude corresponding to one meter, respectively. In advance, one bit is put in front of the integral part of the above result. The bit is zero for east and south and one for west and north.
- **Combine and hash:** The transformation results of the above step are combined by performing a bitwise exclusive-OR operation. Then, MD5 hash algorithm is utilized and generates a 128-bit digest for the combined result. Then, the digest is split into two 64-bit values, called LDEA-keys. This step causes that the target coordinate is unable to be derived from the LDEA-keys.
- **Generate final-key:** A session key (R-key) is generated randomly with the same length of LDEA-key, i.e., 64 bits in the example. LEDA-keys are exclusive-OR with the R-key separately to generate the final-keys. Two final-keys are used as the secret key and initial value of DES symmetric encryption algorithm.

Current design of LDEA algorithm is based on the MD5 hash and DES algorithm. However, LDEA is flexible and can be incorporated with other algorithms, such as AES, triple-DES, etc. These steps should be redesigned when necessary.

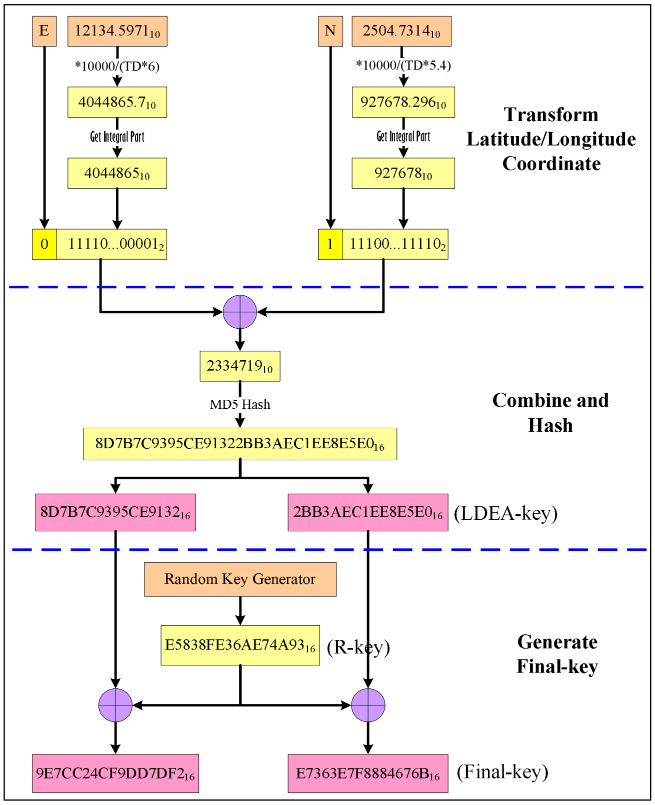


Fig. 2: An example of the final-key generation

SECURITY ANALYSIS AND EXPERIMENTAL STUDY

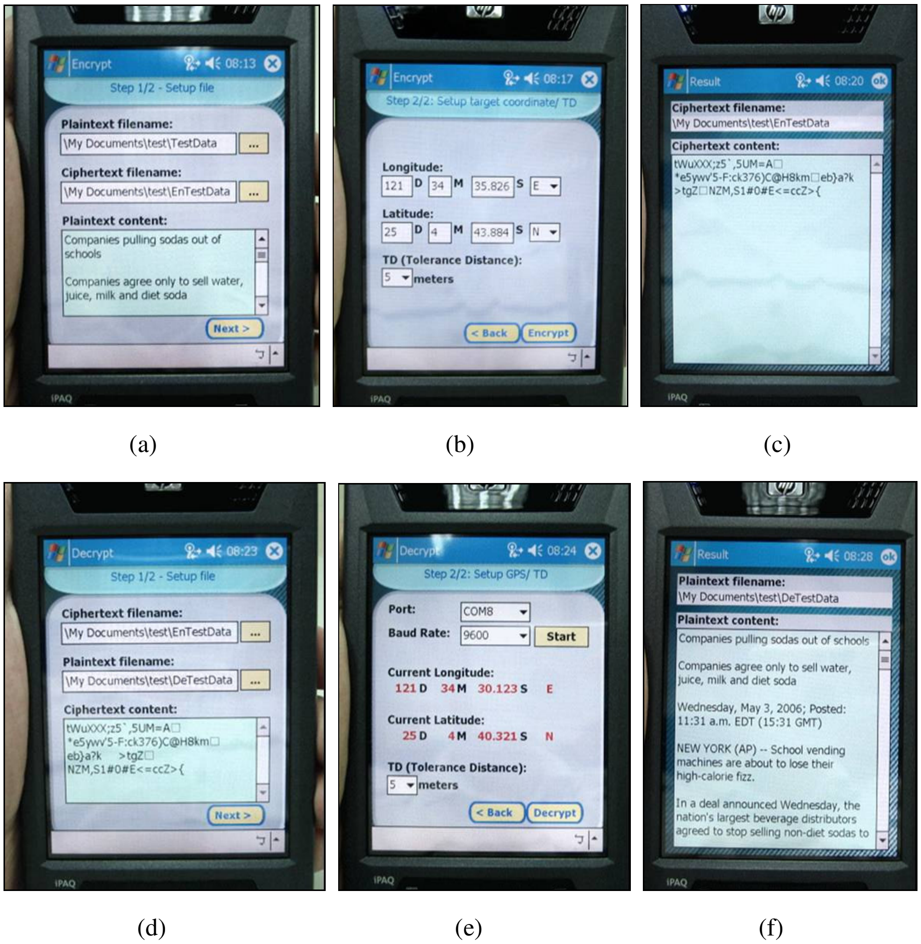
Security Analysis: If the latitude/longitude coordinate is simply used as the key for data encryption, the possible key space is the same as the surface of the Earth that equals 5.11×10^8 square kilometer, i.e., $5.11\times10^{14}\,m^2$. However, 80% of people live on only 3% of the surface on the Earth. If the setting of TD is considered as 20 meters, the probability to break such key is only $1/1.22\times10^{10}$ as shown in Eq. (1). The strength is not strong enough.

$$\frac{1}{5.11\times10^{14}m^2\times0.03/(3.14159\times20^2)m^2}=\frac{1}{1.22\times10^{10}} \qquad (1)$$

That is the reason why a random key is incorporated into LDEA algorithm. The final-key is generated from the exclusive-OR of R-key and LDEA-key. The DES algorithm is used in current design of LDEA and the length of final-key is 64 bits. The probability of breaking the LDEA is $1/2^{64}\,(\approx 1/10^{19})$. Such security strength can be improved by replacing the symmetric algorithm in LDEA.

Experimental Study: A prototype was implemented to illustrate and evaluate the practicality of LDEA algorithm. Six screen shots of the prototype are shown in Figure 3. In Figure 3 (a), the user setups the names of the plaintext and ciphertext files. In Figure 3 (b), the user setups the target coordinate and selects an expected toleration distance (TD). After the ‘Encrypt’ button is pressed, the plaintext file is encrypted and the ciphertext is saved in the ciphertext file as shown in Figure 3 (c).

In Figure 3 (d), the user setups the names of the plaintext and ciphertext files. Then, the coordinate acquired from the GPS receiver is displayed on the screen after user press the ‘Start’ button in Figure 3 (e). The coordinate is used to decrypt the ciphertext file and save the result in the plaintext file. If the acquired coordinate meets the constraint of target coordinate and TD, the content of the plaintext file is the same as the original file as shown in Figure 3 (f). Otherwise, the content is indiscriminate and meaningless.



(a)

Encrypt 08:13

Step 1/2 - Setup file

Plaintext filename: \My Documents\test\TestData

Ciphertext filename: \My Documents\test\EnTestData

Plaintext content:
Companies pulling sodas out of schools

Companies agree only to sell water, juice, milk and diet soda

(b)

Encrypt 08:17

Step 2/2: Setup target coordinate/ TD

Longitude: 121 D 34 M 35.826 S E

Latitude: 25 D 4 M 43.884 S N

TD (Tolerance Distance): 5 meters

(c)

Result 08:20

Ciphertext filename: \My Documents\test\EnTestData

Ciphertext content:
tWuXXX;z5`,5UM=A□
*e5ywv'5-F:ck376)C@H8km□eb}a?k
>tgZ□NZM,S1#0#E<=ccZ>{

(d)

Decrypt 08:23

Step 1/2 - Setup file

Ciphertext filename: \My Documents\test\EnTestData

Plaintext filename: \My Documents\test\DeTestData

Ciphertext content:
tWuXXX;z5`,5UM=A□
*e5ywv'5-F:ck376)C@H8km□
eb}a?k >tgZ□
NZM,S1#0#E<=ccZ>{

(e)

Decrypt 08:24

Step 2/2: Setup GPS/ TD

Port: COM8

Baud Rate: 9600

Current Longitude: 121 D 34 M 30.123 S E

Current Latitude: 25 D 4 M 40.321 S N

TD (Tolerance Distance): 5 meters

(f)

Result 08:28

Plaintext filename: \My Documents\test\DeTestData

Plaintext content:
Companies pulling sodas out of schools

Companies agree only to sell water, juice, milk and diet soda

Wednesday, May 3, 2006; Posted: 11:31 a.m. EDT (15:31 GMT)

NEW YORK (AP) -- School vending machines are about to lose their high-calorie fizz.

In a deal announced Wednesday, the nation's largest beverage distributors agreed to stop selling non-diet sodas to

Fig. 3: The screen shots of the prototype

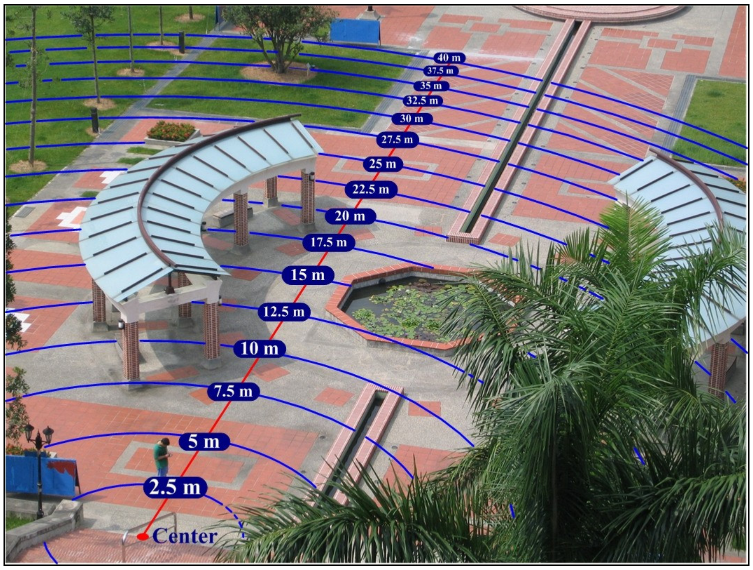


Fig. 4: The design of the experimental site

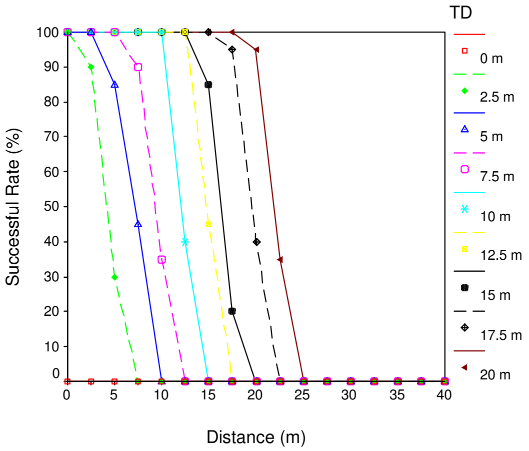


Fig. 5: The successful rate vs. distance under various TD

An experimental site is also designed for the prototype as shown in Figure 4. A set of concentric circles is marked on the ground for every five meters. The center of the circle is defined as the target latitude/longitude location. The settings of TD are 0, 2.5, 5, 7.5, 10, 12.5, 15, 17.5, and 20 meters. The testing distance is from zero to 40 meters for every 2.5 meters. The experimental steps are listed in the following:

Step 1. The target coordinate at the center is acquired from the GPS receiver.

Step 2. For every TD, a source file is encrypted by using the target coordinate and TD firstly.

2a. For every circle, the tester moves randomly along the curve of the circle and tries to decrypt the data about every minute.

2b. There are totally ten times of data decryption. The destination file is checked whether the content is the same as the original file. The number of successful decryption is recorded.

Step 3. Repeat Step 2 until finishing the testing of all TDs.

The successful rate is computed for every combination of TD and testing distance. The experimental result is shown in Figure 5.

In Figure 5, the successful rate of all the testing distance is zero when TD is zero. This is the same as our expectation. The inaccuracy of GPS receiver causes the ciphertext is unable to be decrypted successfully. When TD is five meter, the successful rate is 100% when the tester is at the center. The rate is decreased to 70% when the testing distance is five meters. The maximum distance (MD) is 10 meters when the rate is 0%. It means that the inaccuracy of GPS receiver causes the distance of possible successful decryption may be longer than the setting of TD.

The MDs for every TD are listed in Table 1. The difference of MD and TD is also listed in the table. According to the results, MD is longer than TD about five meters in the experiment. It means that the data can be decrypted beyond the constraint of TD. The user should know such situation. So, the settings of TD should be modified as 2.5+5, 5+5, 7.5+5, and so on. Users can clearly understand that the first number is the TD with almost 100% successful rate and the second number is the extra distance for possibly successful decryption.

Table 1: The MDs under various TDs

Parameters	Values								
TD	0	2.5	5	7.5	10	12.5	15	17.5	20
MD	0	7.5	10	12.5	15	17.5	20	22.5	25
MD–TD	0	5	5	5	5	5	5	5	5
Modified TD	0	2.5+5	5+5	7.5+5	10+5	12.5+5	15+5	17.5+5	20+5

(unit: meter)

CONCLUSIONS

Traditional encryption technology cannot restrict the location of mobile users for data decryption. In order to meet the demand of mobile users in the future, LDEA algorithm is proposed in this paper. LDEA provide a new function by using the latitude/longitude coordinate as the key of data encryption. A toleration distance (TD) is also designed to overcome the inaccuracy and inconsistent of GPS receiver. The security strength of LDEA is adjustable when necessary. The experimental result of the prototype also shows that the decryption is constrained by the range of TD. As a result, LDEA is effective and practical for the data transmission in the mobile environment.

Current design of LDEA algorithm is mainly based on the DES algorithm. Other algorithms, such as AES (Advanced Encryption Standard), triple-DES, *etc.*, can used to replace the DES algorithm when necessary. In advance, the future works may include the following topics:

- The alternative LDEA algorithms incorporating with the mature algorithms can be developed to demonstrate its flexibility.
- Some factors can be incorporated into LDEA, such as time, moving speed, or moving path, *etc.*, to increase the security strength and usability of LDEA.
- The LDEA algorithms can be extended to the other application domains, e.g., the authorization of mobile software. If mobile software is authorized within a pre-defined area, such as a city, the execution of the software may activate the location check based on the LDEA algorithm. The software can be executed only when the user is within the authorized area. Besides, the distribution of multimedia content may be utilized the LDEA algorithm for advanced access control except the

username/password.

The proposed LDEA algorithm provides a new way for data security. It is also meet the trend of mobile computing. Many possible applications will be developed in the future to demonstrate and promote the concept of LDEA algorithm.

ACKNOWLDEGEMENT

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract No.: NSC 94-2815-C-324-007-E

REFERENCES

Aikawa, M., K. Takaragi, S. Furuya and M. Sasamoto, 1998. A Lightweight Encryption Method Suitable for Copyright Protection. IEEE Trans. on Consumer Electronics, 44 (3): 902-910.

Becker, C. and F. Durr, 2005. On Location Models for Ubiquitous Computing. Personal and Ubiquitous Computing, 9 (1): 20-31, Jan. 2005.

Eagle, N. and A. Pentland, 2005. Social Serendipity: Mobilizing Social Software. IEEE Pervasive Computing, 4 (2), Jan.-March 2005.

Gruteser, M. and X. Liu, 2004. Protecting Privacy in Continuous Location-Tracking Applications. IEEE Security & Privacy Magazine, 2 (2): 28-34, March-April 2004.

Jamil, T., 2004. The Rijndael Algorithm. IEEE Potentials, 23 (2): 36-38.

Jiang, J., 1996. Pipeline Algorithms of RSA Data Encryption and Data Compression, In: Proc. IEEE International Conference on Communication Technology (ICCT'96), 2: 1088-1091, 5-7 May 1996.

Lian, S., J. Sun, Z. Wang and Y. Dai, 2004. A Fast Video Encryption Scheme Based-on Chaos. In: Proc. the 8th IEEE International Conference on Control, Automation, Robotics, and Vision (ICARCV 2004), 1: 126-131, 6-9 Dec. 2004.

Liao, H.C., P.C. Lee, Y.H. Chao and C.L. Chen, 2007. A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security. In: Proc. the 9th International Conference on Advanced Communication Technology (ICACT 2007), 1: 625-628, Feb. 2007.

McLoone, M. and J.V. McCanny, 2000. A High Performance FPGA Implementation of DES. In: Proc. IEEE Workshop on Signal Processing Systems (SiPS 2000), 11-13 Oct. 2000, pp: 374-383.

Mohapatra, D. and S. B. Suma, 2005. Survey of Location based Wireless Services. In: Proc. IEEE International Conference on Personal Wireless Comm. (ICPWC 2005), 23-25 Jan. 2005, pp: 358-362.

Mundt, T., 2005. Location Dependent Digital Rights Management. In: Proc. the 10th IEEE Symposium on Computers and Communications (ISCC'05), 2005, pp: 617-622.

Qiu, D., S. Lo, P. Enge, D. Boneh and B. Peterson, 2006. Geoencryption Using Loran. Available at: http://waas.stanford.edu/~wwu/papers/gps/PDF/QiuIONNTM07.pdf

Scott, L. and D. E. Denning, 2003. Using GPS to Enhance Data Security: Geo-Encryption. GPS World, 14: 40-49, April 2003.

Shaar, M., M. Saeb, M. Elmessiery and U. Badwi, 2003. A Hybrid Hiding Encryption Algorithm (HHEA) for Data Communication Security. In: Proc. the 46th IEEE International Midwest Symposium on Circuits and Systems (MWSCAS'03), 1: 476-478, 27-30 Dec. 2003.

Smid, M.E. and D. K. Branstad, 1988. Data Encryption Standard: Past and Future. In: Proc. the IEEE, 76 (5): 550-559, May 1988.

Toye, E. and R. Sharp, A. Madhayapeddy and D. Scott, 2005. Using Smart Phones to Access Site-Specific Services. IEEE Pervasive Computing, 4 (2):60-66, Jan.-March 2005.

Xu, J., B. Zheng, W.C. Lee and D.L. Lee, 2004. The D-Tree: An Index Structure for Planner Point Queries in Location-Based Wireless Services. IEEE Trans. on Knowledge and Data Engineering, 16 (12): 1526-1542, Dec. 2004.

Zhang, Y., W. Liu, W. Lou and Y. Fang, 2005. Securing Sensor Networks with Location-Based Keys. In: Proc. IEEE Wireless Communication and Networking Conference (WCNC 2005), 4: 1909-1914, 13-17 March 2005.

Zhang, Y.P., J. Sun and X. Zhang, 2004. A Stream Cipher Algorithm Based on Conventional Encryption Techniques. In: Proc. IEEE Canadian Conference on Electrical and Computer Engineering (CCECE 2004), 2: 649-652, 2-5 May 2004.