Journal of Education and Science (ISSN 1812-125X), Vol: 31, No: 02, 2022 (94-104)

Improving Security Using Cryptography Based on Smartphone User Locations

Anfal Mahmood Ahmed[1*], Ahmed Sami Nori[2]

[1*,2]Department of Computer Science, College of Computer Science and Mathematics, University of Mosul, Mosul, IRAQ

E-mail: [1*]Anfal.csp40@student.uomosul.edu.iq , [2]ahmed.s.nori@uomosul.edu.iq

(Received March 05, 2022; Accepted April 05, 2022; Available online June 01, 2022)

DOI: 10.33899/edusj.2022.133190.1222, © 2022, College of Education for Pure Science, University of Mosul.

Abstract

Smartphones have become widely employed in a range of fields as a result of substantial developments in communication technology, distribution, and the development of numerous types of smart mobile devices. The goal of this research is to secure information sent over mobile phone networks. In this paper, we propose using cryptography to create a more secure application for transmitting confidential information, using encryption to improve security, and depending on the location of the mobile phone user's coordinates, obtained via GPS, to increase security. The XOR process was used between coordinates, the idea was new, the application was implemented, and good results were obtained. The process of converting text into unreadable text is known as ciphering, and in order to achieve it in this paper the Twofish algorithm was used to encrypt confidential information. When sending the coordinates, the RSA algorithm was used to encrypt them as for the Twofish algorithm, the coordinates serve as a key. We conclude that the proposed system used in this study achieved a high level of security.

Keywords: Cryptography, Twofish, GPS, Smartphone.

تحسين الأمان باستخدام التشفير بناءً على مواقع مستخدمي الهواتف الذكية

انفال محمود احمد[1*] ، احمد سامي نوري[2]

[1*،2] قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة الموصل، الموصل، العراق

الخلاصة :

أصبحت الهواتف الذكية مستخدمة على نطاق واسع في مجموعة من المجالات نتيجة للتطورات الكبيرة في تكنولوجيا الاتصالات والتوزيع وتطوير أنواع عديدة من الأجهزة المحمولة الذكية. الهدف من هذا البحث هو تأمين المعلومات المرسلة عبر شبكات الهاتف المحمول. في هذا البحث ، نقترح استخدام التشفير لإنشاء تطبيق أكثر أمانًا لنقل المعلومات السرية ، وتم استخدام التشفير لتحسين الأمان ، وكذلك اعتمادًا على موقع إحداثيات مستخدم الهاتف المحمول التي تم الحصول عليها عبر نظام تحديد المواقع

العالمي، ولزيادة الامنية تم استخدام عملية XOR بين الاحداثيات ، كانت الفكرة حديثة ، تم تنفيذ التطبيق المقترح وكانت النتائج جيدة. تُعرف عملية تحويل النص إلى نص غير قابل للقراءة باسم التشفير ، وفي هذا البحث تُستخدم خوارزمية تشفير قوية وذات امنية عالية هي خوارزمية Twofish لتشفير المعلومات السرية. عند إرسال الإحداثيات ، يتم استخدام خوارزمية RSA لتشفيرها. بالنسبة لخوارزمية Twofish تم استخدام الإحداثيات كمفتاح. تم تحقيق مستوى عال من الأمن من خلال النظام المقترح.

الكلمات المفتاحية: التشفير، خوارزمية Twofish، نظام تحديد المواقع العالمي، الهواتف الذكية.

---

1. Introduction

Information security appears to be the most essential and required issue in technological growth in order to guarantee the privacy of data when it is transmitted across the network. Cryptography as a term is defined as the art and science of securely converting and transferring private data against third-party attackers. To put it another way, cryptography is the art and science of maintaining security by encoding messages in an unreadable form (unintelligible). The origins of the word come from the Greek terms "crypto" and "graphy" which mean "hidden" and "writing," respectively [1][2].

A cryptographic system's core premise is to encrypt information or data in order to ensure that it remains confidential and that an unauthorized person cannot deduce its meaning. Two of the most popular applications of encryption are to send data across an unsecured channel, such as the Internet, and to ensure that unauthorized persons do not know what they are looking for in a situation where they have access to.

The hidden information is referred to as "plaintext" in cryptography, and the act of masking plaintext is referred to as "encryption"; whereas the encrypted plaintext is referred to as "ciphertext." This is accomplished by using a set of rules known as "cryptographic algorithms." The encryption procedure is usually based on an "encryption key," which is fed into the encryption algorithm along with the data. The receiving side can extract the information using the "decryption algorithm" and the corresponding "decryption key." [3].

Cryptography's fundamental goal is to provide security and the process of encrypting plaintexts was first employed to safeguard national secrets and information. It was quite uncommon in public at the beginning of its use and few people and organizations were familiar with it. However, when banks and financial organizations began conducting transactions online, they needed a mechanism to protect the data, therefore encryption technologies were implemented. Encryption is currently employed in almost every situation where data security is a top issue [4].

The Global Positioning System (GPS) is a space-based navigation system consisting of 24 satellites deployed into orbit by the US Department of Defense. GPS was first used in the military, but it was made available to consumers around the world in 1980. Any industry that requires location, velocity, heading, and timing information nowadays uses GPS. This system has many applications connected with it like navigation, surveying, agriculture, security, mining, and aviation. For military and commercial use, GPS satellite transmitters send out distinct signals [5]. In this research, a technique is given for improving the security of the encryption method for mobile users by exploiting location.

The paper is organized as follows: the first section presents previous works, the second describes the proposed system in detail, the third section focuses on the results and discussion, and section four summarizes the conclusions and findings of this paper.

2. Related Works

In 2015, Khoshali and Varsha introduced a steganography methodology that uses audio files as cover signals to conceal sensitive/confidential data. Furthermore, the site has been considered for increased data security and GPS tracking. The proposed system is powerful in sound and audio signals effectively. The model achieves strict security measures [6].

In 2015, Apurfa et al. developed a banking application using location-based cryptography. This means that in cryptography only a certain site can decrypt the ciphertext. When attempting to decrypt the data at a different location, the decryption process fails, and no clear text information is shown. LDEA was employed by the authors [7].

In 2015, Aniruddha et al. developed a method to increase the security of an encryption algorithm by tracking the location of a mobile phone using the Global Positioning System (GPS). They propose a solution that an encrypted file can only be decrypted by being in a specific place determined by the user who encrypts the file.

The authors used the AES algorithm and concluded that by using the location and other data such as date and time, they may improve the security of a method [8].

In 2015, for secure communication, Pranjala introduces the concept of "geocoding" based on location which focuses on the attempts to improve the existing AES-GEDTD technique, which has difficult computability and greater cost, by developing M-AES-GEDTD; a new algorithm with lower complexity and cost [9].

In 2017, Gaikwad et al. created a method for protecting data transmission by encrypting the data to be transferred and using the concept of geo-encryption, or location-based encryption, to limit the location of the data to be transmitted. The sender provides a file location and the receiver's time at the time when the data will be decrypted, and the encryption and decryption procedure is done using the AES algorithm, and the encrypted message is transferred. To decode the message, the recipient must be present at the stated location and at the specified time. Message decoding occurs only if the user is present at the stated location and time; otherwise, the message is not decoded [10].

In 2017, Lin You et al. present a new location-based encryption model based on a fuzzy vault approach. After deciding on an encryption algorithm, they used a fuzzy vault approach based on a location-based digital fingerprint to keep the secret key safe. They used location data captured by the users' mobile devices and created a fuzzy vault to securely store both the digital fingerprint and the secret key [11].

Due to the advancement of mobile phone networks and GPS technology, in 2018, Sriram et al. concentrated their study on the idea that a location-based data encryption method and decryption is in a specific spot, where they used the location as an extra security feature [12].

In 2020, Nur and Sakinah offered an improved technique in android application development that encrypts data before sending it to cloud storage using location-based encryption, as well as a secret keyword to handle the upload and download process during the hashing function to safeguard the keys held in cloud storage. Due to its high performance, the AES method was used to encrypt and decode data with location coordinates as an additional encryption key known as the geo-lock key. The use of location information to construct the key ensured that the decryption procedure would only take place at the given location before the encryption process began [13].

3. Proposed System

3.1. Android

Android is a Google-developed mobile operating system that is primarily geared for touchscreen mobile devices such as smartphones and tablets. Android smartphones have a higher number of devices

than any other smartphone. Android is significantly more powerful than any other operating system, including Apple iOS and BlackBerry, and it is supported by a large number of device makers all over the world [14].

3.2. Twofish Algorithm

Bruce Schneier, an American cryptographer, initially released The Two Fish in 1998. The two fish algorithm is a block cipher that uses a 128-bit plaintext as well as a key length of 128, 192, or 256 bits [15].

Twofish is a symmetric block cipher that handles the 128-bit input message as blocks with a key. It stands out for its sturdy keys and versatile design. It is cost-effective in respect of both hardware and software, and it can be used on a variety of systems. It is also suitable for stream ciphering. Twofish's main work is built on the Feistel network, which has 16 iterations [16].

The algorithm of Twofish was created with simplicity in mind. The efficiency of Twofish, on the other hand, is primarily dependent on hardware (in terms of CPU power and/or VLSI technology). There is presently no lucrative cryptanalysis of Twofish [17][18].

Some of the main components of the Two fish algorithm are as follows:

1- Feistel: In a block cipher, Feistel is a general method for converting any function F into a permutation. It was created by Horst and was first utilized in the DES algorithm. It divides the input block into two sections and repeats the same activities.
2- Substitution Boxes (S-Box): The S-box is a table-driven non-linear substitution process with variable input and output sizes. It can be made in one of two ways: randomly or via an algorithm. Twofish makes use of four different S-boxes, each made up of two fixed 8-by-8-bit permutations and key elements.
3- MDS Matrices: The MDS matrix is a 4x4 matrix that enables diffusion, with the MDS code defined as a linear mapping between the elements of two fields (a and b) to form a composite vector (32 bits) of elements (a + b). Using the irreducible polynomial x8 + x6 + x5 + x3 + 1, this matrix is used to multiply four-byte vectors in the GF (28).
4- Pseudo-Hadamard Transforms (PHT): A PHT is a simple diffusion blending. Given two inputs a and b, the 32-bit PHT, for example, is defined as follows:
   $a' = a + b \bmod 2^{32}$
   $b' = a + 2\,b \bmod 2^{32}$
5- Whitening: Before the first round and after the last round, plain-text parts are combined with key components using XOR to increase the key's security versus assaults [16].
6- Q-Permutation: The Q-Permutation is at the core of Twofish's design. The fixed permutations q0 and q1 are based on 8-bit integers. The S-boxes' main components are these permutation functions [12].

3.3. RSA algorithm

The RSA (Rivest-Shamir-Adleman) cryptography algorithm is asymmetric. The Massachusetts Institute of Technology's Ton Rivest, Adi Shamir, and Leonard Adleman were the first to officially reveal RSA through 1977. In RSA cryptography, both the public and private keys can be used to encrypt a message; the opposite key used to encrypt the message is used to decrypt it. This is one of the reasons why RSA is the most widely used asymmetric algorithm [19].

The production of public and private keys is the most difficult aspect of RSA cryptography. The difficulty of factoring in huge prime numbers is what gives RSA its security [20].

3.4. The process of generating keys

1. The sender's and recipient's coordinates are first collected using a GPS smartphone.
2. XOR operation is performed between the coordinates of the sender and receiver and the result will be the key to the Twofish algorithm.

3.5. Text encryption algorithm

1- The key generated from the coordinates of the sender and receiver is used as a key to the algorithm, through which the keys are initialized for the algorithm.
2- The secret text to be encrypted is entered.
3- The text to be inputted should be 128 bits in length; if it is less, its zeros are inserted; if it is more than 128 bits, it is divided into groups, each of which is 128 bits in length.
4- The system will produce R0B, R1B, R2B, and R2B, R0B which is the first four bytes of the text, then we will convert the bytes into long, and then a XOR will be made with the keys K0, K1, K2, and K3 will produce R0, R1, R2, and R3.
5- F-Function will have R0 and R1 placed into it, producing in F0 and F1.
6- After that, a XOR is performed between F0 and R2 to generate C2, which is then rotated to the right.
7- The R3 is then rotated to the left, and the XOR between R3 and F1 is performed, yielding C3.
8- We Will produce R0, R1, C2, and C3, and then the switching process will be produced, and C2, C3, R0, and R1 will be produced.
9- As of now, this has only been for one round; after that, the output undergoes a whitening procedure, i.e., the XOR operation with K4, K5, K6, and K7.
10- Until the text is produced, they will be converted from long to bytes and then added to the Result array and the ciphertext is produced
11- The end.

Figure (1) shows the encryption process.

3.6. Text decryption algorithm

1- The key generated from the coordinates of the sender and receiver is used as a key to the algorithm, through which the keys are initialized for the algorithm.
2- The Ciphertext to be decrypted is entered.
3- The Ciphertext to be decided to enter should be 128 bits in length; if it is less, zeros are appended; if it is larger than 128 bits, it is divided into groups of 128 bits each.
4- Will produce R0B, R1B, R2B, and R3B, R0B which is the first four bytes of the text, then we will convert the bytes into long, and then a XOR will be made with the keys K4, K5, K6, and K7 will produce R0, R1, R2, and R3.
5- At first, the process of switching to R0, R1, R2, and R3 is done, as shown:

Br 0=R0
Br1=R1
R0=R2
R1=R3
R2=Br0
R3=Br1

6- Then the R0 and R1 are entered into the F-Function, resulting in F0 and F1
7- R2 is rotated to the left and then XOR is made for it with F0.
8- A XOR is made between R3 and F1 and then the output is rotated to the right.
9- As of now, this has only been for one round; after that, the output undergoes a whitening procedure, i.e., the XOR operation with K0, K1, K2, and K3.
10- Until the text is produced, they will be converted from long to bytes and then added to the Result array and the plain text is produced
11- The end

Figure (2) shows the decryption process.

4. Discussions and Results

The Android Studio Platform was used to execute the project, which was written in Java. The sender's location is initially identified using the smartphone's GPS, and then the position is communicated with the receiver via a social media program during transfer; the coordinates are encrypted using the RSA technique, so the sender's coordinates will arrive at the receiver encrypted**.** In the same way, the recipient shares his/her location with the sender, and when sending, the coordinates are encrypted by the RSA algorithm. Then the coordinates are decrypted and the XOR operation is used between the coordinates of the sender and the receiver, and the output of the XOR operation will be the used key for the encryption algorithm, as shown in Figure 3. After entering the secret message, we have to click on the encryption button (Encrypt).

The secret message will be encrypted by the Twofish algorithm and using the key generated by the coordinates as in Figure 4.

When the text Decryption is in process, the recipient enters its encrypted coordinates and the sender’s encrypted coordinates to obtain the decryption key and then clicks on the decrypt message button (Decrypt), and the secret message is obtained as in Figure 5.

Tables 1, 2, and 3 represent the results of performing the process of encrypting with different sizes of text and have used different key lengths with 128-bit,192-bit, and 256-bit respectively. In general, the results were good.

Table 1: Execution time and throughput results for the encryption and decryption process when key length is 128-bit

Size of Plain-Text (KB)	Execution time for encrypting process in m.s	Size of Cipher-Text (KB)	Execution time for decrypting process in m.s
0.935	199	0.944	205
1.052	228	1.056	202
1.169	223	1.184	245
1.871	345	1.872	385
2.807	562	2.816	502
Average Time	1.557	Average Time	1.539
Throughput(KB/ms)	5.03	Throughput(KB/ms)	5.11

Table 2: Execution time and throughput results for the encryption and decryption process when key length is 192-bit

Size of Plain-Text (KB)	Execution time for encrypting process in m.s	Size of Cipher-Text (KB)	Execution time for decrypting process in m.s
0.935	185	0.944	232
1.052	212	1.056	217
1.169	238	1.184	230
1.871	395	1.872	359
2.807	554	2.816	556
Average Time	1.584	Average Time	1.594
Throughput(KB/ms)	4.94	Throughput(KB/ms)	4.93

Table 3: Execution time and throughput results for the encryption and decryption process when key length is 256-bit

Size of Plain-Text (KB)	Execution time for encrypting process in m.s	Size of Cipher-Text (KB)	Execution time for decrypting process in m.s
0.935	187	0.944	206
1.052	230	1.056	198
1.169	251	1.184	234
1.871	380	1.872	364
2.807	525	2.816	527
Average Time	1.573	Average Time	1.529
Throughput(KB/ms)	4.98	Throughput(KB/ms)	5.14

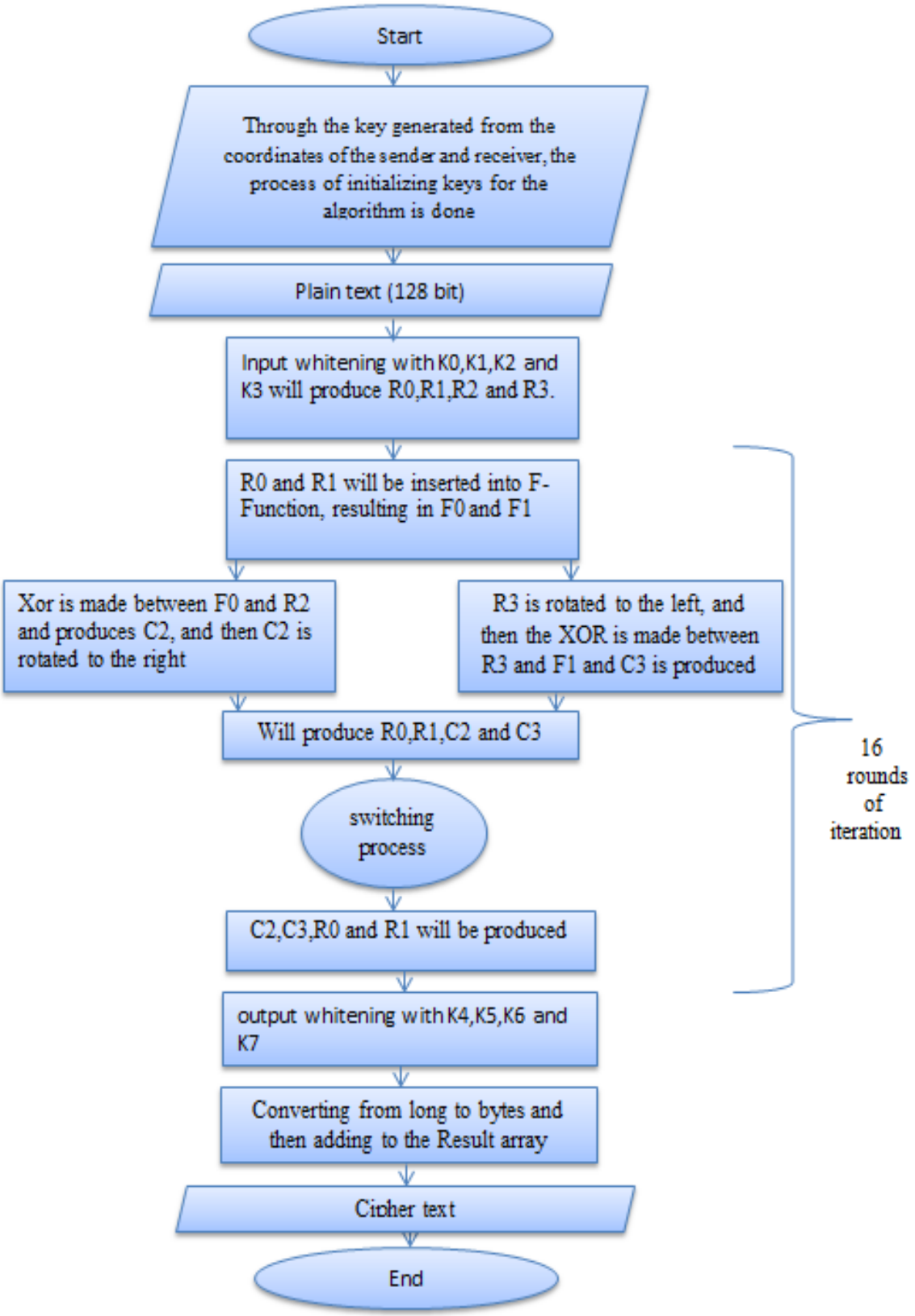

Fig. 1. The Process of Encryption Text.

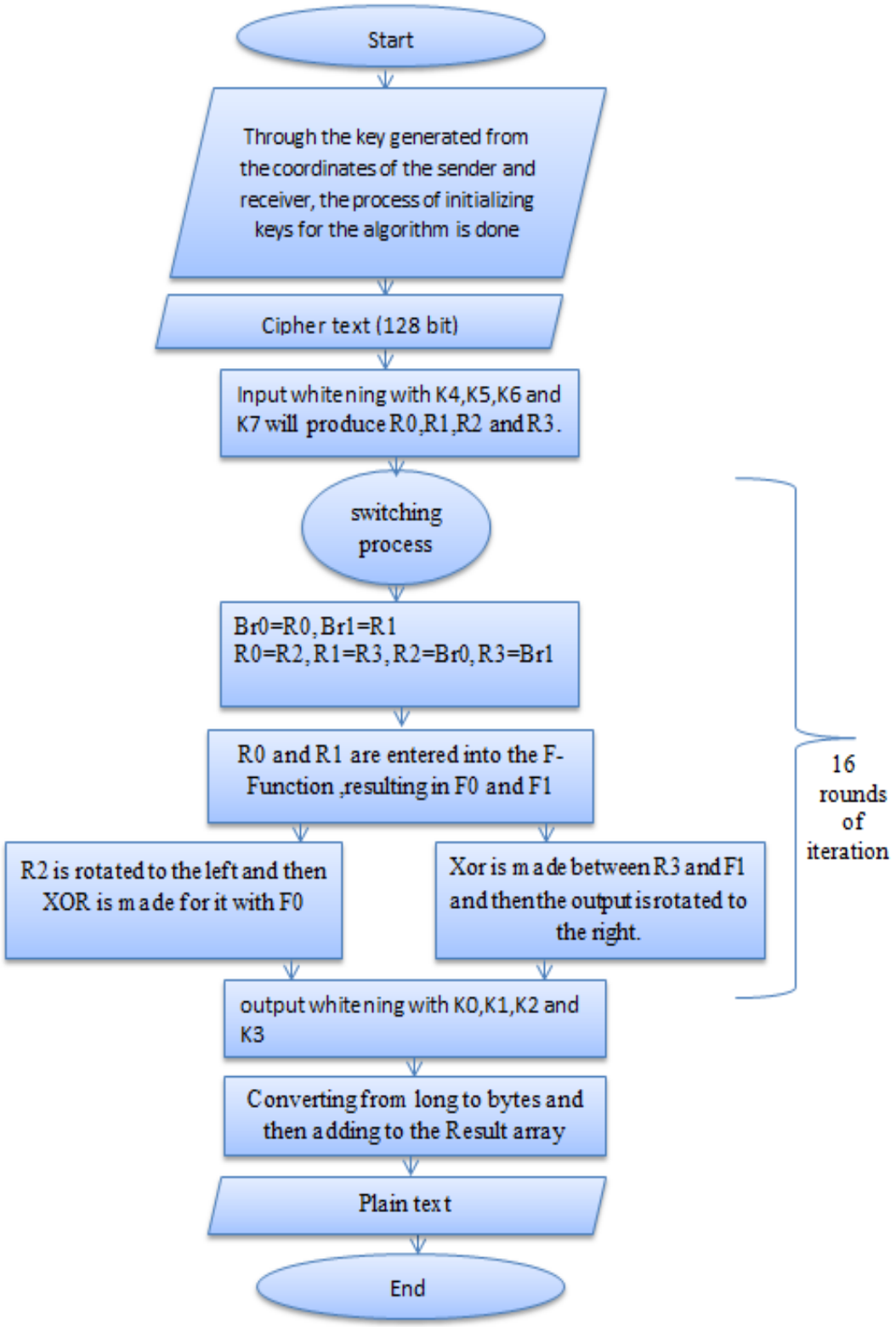

Fig. 2. The Process of Decryption Text.

Fig. 3. Coordinate Determination Interface.

Fig. 4. Text Encryption Interface.

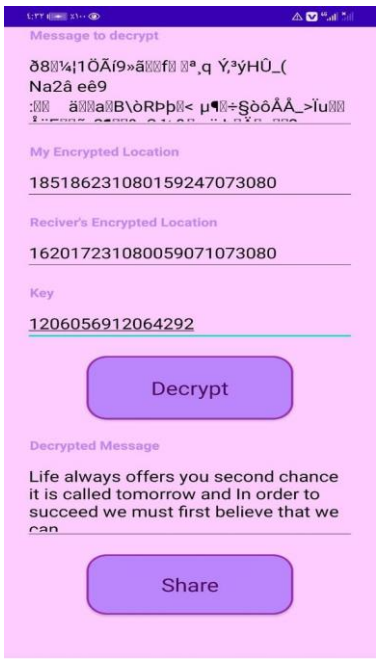

Fig. 5. Cipher-text decrypting Interface.

5. Conclusion

The proposed system accomplished excellent security by utilizing GPS technology to collect the sender and recipient's locations and used the RSA algorithm to encrypt the coordinates during transmission, as well as a XOR operation between the two positions to obtain the algorithm key. The system has achieved enhanced security for the encrypted confidential data by using encryption techniques through using the proposed approach for encrypting the text. This paper concludes that the suggested system addresses the major concerns about safeguarding information received over mobile networks, resulting in a high level of security.

For future studies, we suggest the following: Use another equation or other method between the coordinates to generate the algorithm key. Use another technique with encryption technology, for example, steganography technology, and this will lead to increased security as a result of combining the two technologies.

6. Acknowledgements

The authors are grateful to the Department of Computer Science at the University of Mosul/Iraq for all the support that allowed this study to materialize.

7. References

[1] P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, "Efficient data security using hybrid cryptography on cloud computing," in *Inventive Communication and Computational Technologies*, Springer, 2021, pp. 537–547.

[2] M. O. Asanbe, "Hybrid Data Security: A Review of Cryptography And Steganography Techniques," *Villanova J. Sci. Technol. Manag.*, 2019.

[3] A. M. Qadir and N. Varol, "A review paper on cryptography," in *2019 7th international symposium on digital forensics and security (ISDFS)*, 2019, pp. 1–6.

[4] F. Abbasi and P. Singh, "Cryptography: Security and Integrity of Data," *J. Manag. Serv. Sci-ence*, vol. 1, no. 2, p. 4, 2021.
[5] Z. Haider and S. Khalid, "Survey on effective GPS spoofing countermeasures," in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, 2016, pp. 573–577.
[6] K. Pandit and V. Bhosale, "Implementation of Location based Steganography on mobile Smartphone using Android Platform," *Int. J. Comput. Sci. Inf. Technol.*, vol. 6, no. 3, pp. 2606–2609, 2015.
[7] A. Deshpande, M. Jagtap, S. Kadam, A. Chechare, and P. Dhade, "Security to mobile banking using location based encryption," *Int. J. Adv. Res. Comput. Eng. Technol*, vol. 4, no. 11, pp. 4011–4014, 2015.
[8] A. S. Raut, H. N. Shinde, S. R. Vidhale, R. V Sawant, and V. A. Kotkar, "Enhancing Security using Location of Mobile Users."
[9] P. G. Kolapwar, "An improved geo-encryption algorithm in location based services," *IJRET Int. J. Res. Eng. Technol*, vol. 4, no. 5, pp. 547–550, 2015.
[10] P. S. Gaikwad, P. Dalvi, M. Patel, C. Dhalpe, and A. Chaudhari, "MOBILE APPLICATION FOR PROVIDING SECURITY TO DATA TRANSMISSION."
[11] L. You, Y. Chen, B. Yan, and M. Zhan, "A novel location-based encryption model using fuzzy vault scheme," *Soft Comput.*, vol. 22, no. 10, pp. 3383–3393, 2018.
[12] G. Sriram, B. Srikanthreddy, K. V. Seshadri, K. Hemantha Kumar, and N. Suresh, "Location based encryption-decryption system for android," *Proceedings of the International Conference on Smart Systems and Inventive Technology, ICSSIT 2018*. pp. 590–593, 2018, doi: 10.1109/ICSSIT.2018.8748555.
[13] N. S. M. Shamsuddin and S. A. Pitchay, "Implementing location-based cryptography on mobile application design to secure data in cloud storage," in *Journal of Physics: Conference Series*, 2020, vol. 1551, no. 1, p. 12008.
[14] A. Ullah and M. Ijaz, "Stego App: Android based Image Steganography Application using LSB Algorithm," *Int. Res. J. Eng. Technol.*, vol. 5, no. 9, pp. 862–865, 2018.
[15] A. Devi and B. S. Ramya, "Two fish Algorithm Implementation for lab to provide data security with predictive analysis," *Int. Res. J. Eng. Technol.*, vol. 4, no. 5, pp. 3033–3036, 2017.
[16] S. M. Kareem and A. M. S. Rahma, "A novel approach for the development of the Twofish algorithm based on multi-level key space," *J. Inf. Secur. Appl.*, vol. 50, p. 102410, 2020.
[17] A. Ghosh, "Comparison of encryption algorithms: AES, Blowfish and Twofish for security of wireless networks," *Int. Res. J. Eng. Technol.*, vol. 7, pp. 4656–4658, 2020.
[18] G. Dhamodharan, S. Thaddeus, L. C. Flores, J. L. Hilario-Rivas, and F. Sandoya, "Embedding Elliptic Curve Cryptography and Twofish Algorithm to Improve Data Security in Internet of Things," *Adv. Mech.*, vol. 9, no. 3, pp. 971–978, 2021.
[19] R. F. S. L. Et.al, "Improvement of RSA Algorithm Using Euclidean Technique," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 3. pp. 4694–4700, 2021, doi: 10.17762/turcomat.v12i3.1889.
[20] P. K. Kalabhavan and B. Bodheswaran, "A Novel Approach for Encryption and Decryption by RSA Algorithm in Secure Multimedia Communication," vol. 4, no. 6. pp. 254–256, 2021.