LBS Steganography Method an Mobile Image Based on NTRU Algorithm

Ass.Lecturer.Zainab khyioon Abdalrdha

Computer Science Department ,University of Mustansiriyah

Baghdad, Iraq

E-mail:zainabkhyioon83@yahoo.com

Tel: ٠٧٧٢٢٦٣١١٤٥

Mushtaq Talib Ajjah

Huda Abdul-alteef Abdul-ijabbar

Computer Science Department ,University of Mustansiriyah

Baghdad, Iraq

E-mail:altaib.mushtaq @yahoo.com

Abstract

Due to wide spread use of mobile phone and more available applications like the internet. The Internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. The important of reducing a chance of the information being detected during the transmission is being an issue now days.

In this paper steganography method based on Least Significant Bit (LSB) is used. The technique that are optimized by XOR method which increases the security of the text before it send across the medium to hiding messages in an image and increase the confidentiality by using NTRU (Nth degree truncated polynomial ring units) algorithm to provide cipher text that can be recovered. The proposed system in this paper is made by using programming language JAVA version 7, Android operating system version (4.2) and it was designed for color image was

sent by Viber, Whats App, and E-mail programs thus making it harder for unauthorized people to extract the original message. The proposed approach is tested using different types of mobile phones (Galaxy S3, Galaxy S4, HTC).

Keywords: Cryptography, NTRU Algorithm , Steganography, Android Operating System.

تقنية الاخفاء(LSB) لصور مبايل اعتمادا على خوارزمية NTRU

الخلاصة :

بسبب الانتشارالواسع لأستخدام النقال وتوفرالتطبيقات الكثيرة مثل الانترنيت والإنترنت ككل لا يستخدم وصلات آمنة،وبالتالي فان المعلومات في النقل قد تكون معرضة لاعتراض الاهمية .لتقليل التغير الحاصل للمعلومات التي تم اكشافها خلال عملية النقل.

في هذا البحث سوف نركز على تقنية الاخفاء (Steganography) بواسطة استخدام تقنية البتات الأقل أهميه "LSB" والتي تم تحسينها عن طريق استخدام طريقةXORالتي تزيد السرية والتعقيد للرسالة قبل الإرسال عبرالوسط لأخفاء الرسائل في الصورة وزيادة السرية بواسطة استخدام خوارزمية NTRU لتوفير النص المشفر الذي يمكن استرجاعه.النظام المقترح في هذاالبحث تم كتابته بواسطة اللغة البرمجية (Jave)اصدار ٧ ونظام تشغيل (Android) اصدار (٤,٢)، وهومصمم للصورالملونة وتم إرسال هذه الصورة عبر برامج Viber, WhatsApp ,and E-mail وهذه العمليات أعطت نتائج جيدة ونوعية الصورة لم تتأثر خلال هذه العمليات.

مفتاح الكلمات : التشفير لكتابة المشفرة، خوارزمية NTRU ,الاخفاء , نظام تشغيل الاندرويد

1. Introduction

The idea of Information Hiding can be traced back to a few thousand years ago. In many Competition environments, hide the presence of communication is desirable to avoid suspicion from adversaries [1].They represent a class of operation used to embed data into different forms of media such as images, sound, or text. The embedded data should be invisible to any observer [2]. In the past few years there has been growing interest in ways to quickly hide the information with other information. The fact that an unspecified number of copies can be produced illegally, Led to a study of ways to embed copyright information hidden serial the preparation of audio and video data; the concern that privacy could be eroded led to the retransmission of unknown services systems, and techniques for making laptops difficult for a third party to track. Restrictions on some governments provide encryption to drive people to study and find ways to services for those who communicate secretly [3]. Hide information is technology include confidential information to data covering, make confidential information invisible or inaudible to any observer [4]. The cryptography and steganography both give the total security to a data or information, thus we need to apply both techniques to achieve essential security. There are number of ways can be done, but here we will concern with methods of altering the information contained in such a way that the recipient can undo the alteration and discover the original data [5]. Steganography and cryptography are two related areas. Cryptography dissolves the message so it cannot be understood; As long as the secret key is unknown, so it cannot recover the original message. Steganography hides the message so that we cannot see them or detected [6].

2. Mobile phone

Mobile phones or hand phone is a form of communication that relies on wireless connectivity through a network of distributed transmission towers inside secure area. The hand phones evolution has meant her to be not only a way voice communication [7]. However, they have begun be used as minimal computer machine to send and receive

emails messages, designation, and surfing web. Also, the best developed and capable of capturing images that are compared with high- precision cameras. Hand phone have become a way to boost advertising, because of competition from the service provider to increase mobile phones, communication has become the price of using these telephone at high price and a wide range of human [8].

3. Cryptography

Process of concealing information and the operation of camouflage it, is known as encryption. The encrypted original text is called the cipher text and a collection of rules used to encrypt information from the ordinary is encryption algorithm. Usually run this algorithm based on the key of encryption, which is a contribution to the algorithm along with the letter. In order to enable the receiver to get the letter of the cryptogram there has a decryption algorithm which, when used with the suitable key of decryption, return the original text of the cipher text [9]. The cipher system is shown in figure (1).

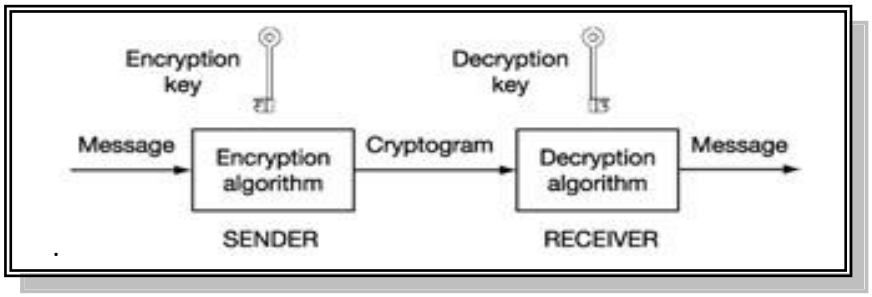

Figure (1) Cipher system

The encryption is the best effective way to accomplish security of data means. Encryption method hides the contents of the original letter can be retrieved through the decryption method [10]. The primary purpose from encryption is to prevent unauthorized from seeing or modify data. Algorithms depend on key use key to encrypt the letter. There are two general categories depend on encryption key :**symmetric encryption** which work with a single key to encryption and decryption the letter, and **asymmetric encryption** which work with two contrast keys: two public

and private keys one for encoding letter, and other for decoding it [11].In this paper used NTRU is the latest in the line of Public Key Cryptographic Systems. It is relatively new and was conceived by Jeffrey Hoffstein, Jill Pipher and Joseph. H.Silverman. NTRU uses polynomial algebra combined with the clustering principle based on elementary mathematical theory. The security of NTRU comes from the interaction of polynomial mixing modulo two relatively prime numbers. The mathematics which used in NTRU is based on lattice-based cryptography it has different cryptographic properties from RSA (Rivest, Shamir and Adleman) and ECC (Elliptic Curve Cryptography)[12].

3.1 Description of NTRU Public Key Cryptosystem

The NTRU cryptosystem can be used in a range of application which involves security in a network. NTRU is depending upon the algebraic structures of certain polynomial rings. The NTRU Encrypt is a public-key cryptosystem which is based on the shortest vector problem in section illustrated NTRU algorithm in details.

3.1.1 NTRU Public Key Cryptosystem Parameters

NTRU stands for Number Theory Research Unit. NTRU is actually a parameterized family of cryptosystems; each system is specified by three integer parameters (N, p, q) which represent the maximal degree N-1 for all polynomials in the truncated ring R, a small modulus and a large modulus, respectively, where it is assumed that N is prime, q is always larger than p, and p and q are co-prime. The NTRU algorithm involves three steps: key generation, encryption and decryption, throughput [13].

1. NTRU Key Generation

Key Generation-NTRU involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the NTRU algorithm are generated the following way:

User B wants to create a public/private key pair for the NTRU [14] PKCS. B first randomly chooses two small polynomials f and g in the ring of truncated polynomials. A small polynomial is small relative to a random polynomial *mod q*. In a random polynomial the coefficients are

much smaller than ***q***. B must keep the values of the Polynomials ***f*** and *g* private, since anyone who knows the value of either of them will be able to decrypt messages sent to B. B's next step is to compute the inverse of the f modulo q and the inverse of f modulop. Thus B computes polynomial fp and fq with the property that ***f*fq = 1 (modulo q)***and ***f*fp = 1 (modulo p)***.If by some chance if the inverse does not exist, B will need to go back and choose another f. For information about computing inverses in the ring of truncated polynomials ,User B chooses two polynomials f and g, where polynomial ***f*** is invertible polynomial. B keeps the polynomials *f* and *g* private and generates a public key has follows:

h=p fq*g(mod q)
Here ***fq***is ***f-1(mod q)*** **or** ***f*fq(mod q)=1***.

B's private key is the pair of polynomials *f* and *fp*. B's public key is the polynomial *h*.

2. NTRU Encryption
The NTRU Crypto-system is based on three parameters p, q and N where p is a small prime number and q and p are relatively-prime and N is the degree of the polynomial in the ring of polynomials. When User A wants to send a message to User B, Aconverts the message to the form of binary polynomial m(which is of the same order as f and g). A uses B's public key and generates the cipher text e as follows: e=h*r +m (mod q), where r is any small polynomial too bscure the original message m[14].

3. NTRU Decryption
User B has received A's encrypted message e and Bwants to decrypt it. B begins by using the private polynomial f to compute the polynomial = f*e (mod q)= f*(h*r +m) (mod q)=f*(pfq*g*r* +m)(mod q)= pg*r +f*m
Since B is computing a modulo q can choose the coefficients of a to lie between -q/2 and q/2. In general B will choose the coefficients of a to lie in an interval of length q. The specific interval depends on the form of the small polynomials. It is very important that B does this before performing the next step. B next computes the polynomial = a(mod p) = f*m
That is, B reduces each of the coefficients of a modulo p.
Finally B uses the other private polynomial fp to compute
C = fp *B (mod p) = fp * f * m (mod p) = m
The polynomial c will be A's original message m[14].

4. Steganography

Steganography is derived from two words "Steganos" and "Graphia" means "covered" or "hidden" and "written" respectively [15]. The main purpose of this technique is using for hiding data in a cover media therefore data is undetectable by anyone else. The simple implementation method of this technique is use to hide text data in cover image file. The cover media for a steganography technique can be a text, audio, image or video. Mostly text steganography is not used as it contributes in increasing the difficulty level of detecting of hidden bits, while text cover data offers smaller memory occupation and is simpler to communicate [16]. Steganography add another layer of secrecy **undetectability** over cryptography **confidentiality** [17]. Three factors were used in design method of steganography: perceptual robustness, transparency, and the ability to hide. These requisites are known as "magic triangle" and contradictory [18].

One of the main goals of steganography is perceptual transparency, which means that nobody will notice the existence of hidden information. Therefore, in steganography methods, if someone knows that there is a piece of hidden information, usually he/she can extract it easily. This is the major distinction between steganography and other methods of hidden exchange of information [19]. Steganography is one of the most popular ways for secret communication. In steganography secrete message can be hidden in voice, video, text and image [20]. Steganography different from cryptography in the feel that that wherever concentrates cryptography to keep secret of message contents, steganography focused on maintaining a secret message. Each of steganography and coding is a way to safeguard the information as of unauthorized persons, but technology alone is not ideal, so need to can be unwound. Once revealed the existence of hidden information, and defeated the purpose of concealing information partially [21]. The power of steganography can amplify through a combination of it with encryption. A basic model for steganography as offer in Figure (2), consists of the following: - [22, 23]

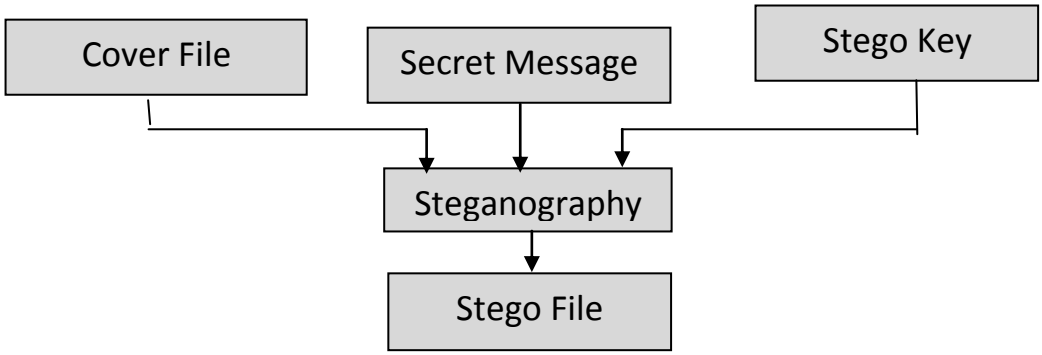

Figure (2) Basic Model of Steganography.

• Cover file (Carrier): is the original file that `an integral part of the secret message required. It is known as host file.
• Payload (Secret Message): Massage is a secret that should be an integral part of the inside cover of a file in a specific steganography model. Load can be text, sound, image [24].
• Stego file (stego-object): is obtained on end file after load included to cover a particular file..
• Stegokey: is the key that might used to code of confidential information for additional level of safety

5.Android Operating System

Android is operating system open source of mobile using for all phones and devices that contain personal computers. Factory can be used a telephone Android if followed the Convention on which came in the field of software development Kit. There are no limitations or conditions on the manufacturers of the telephone company to exchange their extensions with anyone else, as there are in other open-source software, if they leave the of the Linux kernel as it is. Linux kernel under various license and over limitations than Android. Android is a software environment not a hardware platform, which contains an OS, built on Linux Kernel based OS hosting the Dalvik Virtual Machine. The Dalvik Virtual Machine runs Android applications as virtual machine instances. Android has a rich user interface, the application framework, JAVA class libraries, and multimedia support. Android also comes with built in applications contacting features such function of short messaging service (messages); Android software environment is shown in figure (3) [25].

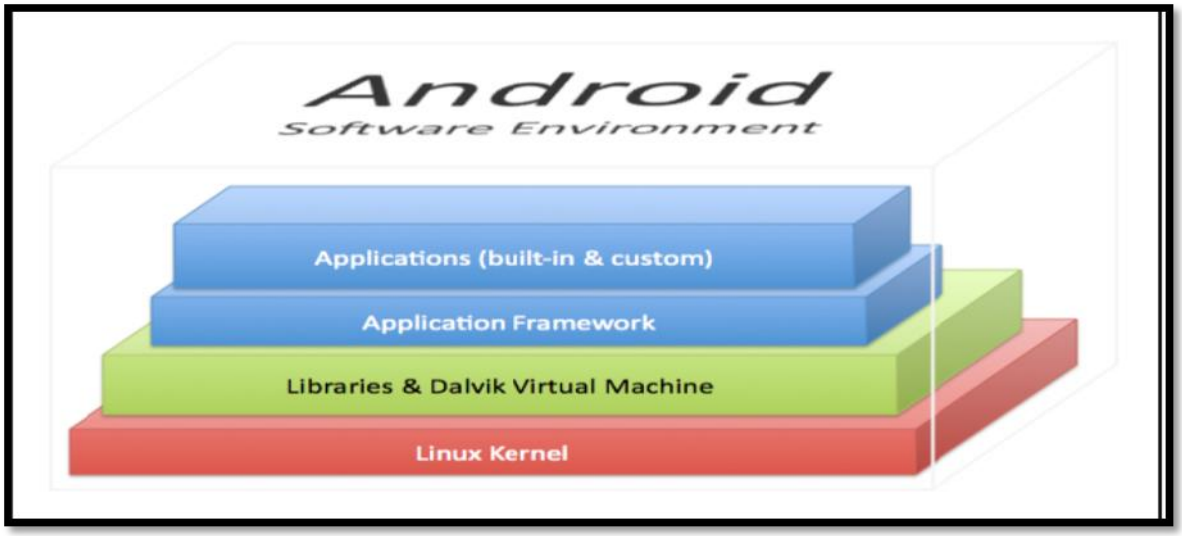

Figure (3) Android Software Environment

6. The Proposed Approach

This section illustrates the proposed Approach for system.

6.1Algorithm to encryption text

In this stage entered text will be encrypted by using NTRU algorithm. The NTRU cryptosystem can be used in a range of application which involves security in a network. NTRU is depending upon the algebraic structures of certain polynomial rings. The NTRU Encrypt is a public-key cryptosystem which is based on the shortest vector problem. Its main characteristics are the low memory and computational requirements as providing a high security level. It is a very well-organized public-key cryptosystem based on polynomial arithmetic.

6.2 XOR Method to hiding text

XOR operator very common ingredient in more complex ciphers. In itself, using a constant repeating key, a simple XOR codes can trivially be broken by using hesitate analyze. If the content of any message can be guessed or otherwise known then the key can be detect. In steganography the hidden information is important, Steganography is to conceal the message in such a method that no one but the sender and the receiver knows of the survival of the letter. An approach is different from the encoder, which aims to make the information not readable. The embedding process is achieved by converting cipher text “the result of

encryption operation" to binary and then using password (As the key to the way XOR) and repeat the password on the length of the cipher text. XOR method test of cipher text and then decides 0 or 1 to be an integral part. XOR is known as 'Exclusive-OR' and it is a bitwise operator from binary mathematics. Uses operator XOR for "flip" bits (zeroes and ones) in a piece of regular text to create a encrypted text. Return XOR operators (1) when the value of either the bit the first or second bit is (1). The XOR operators return (0) when either or both of the bits are (1).

The XOR operator is Is a very common ingredient in more complex ciphers. A simple repetition XOR codes is therefore sometimes used to hide information. Eventual embedding starts by embedding the result from XOR operation into the image and beginning from location 100 of pixel by using Least Significant Bit (LSB). LSB insertion is a common and simple approach to embed information in a cover image in sequence. The message stored in the LSB is pixel of the RGB value.

The main difference of the proposed code is the fact that data is now one dimensional array of integer. One integer from this array is associated with each pixel. This integer is 32 bits wide, so it has the capacity to hold the 8-bit red, green and blue components of a pixel value. The remaining 8 bits are used for the alpha component, which represents pixel transparency, and this part of alpha is used to hide information inside the proposed system. The ordering of red, green, blue and alpha is shown in Figure (4).

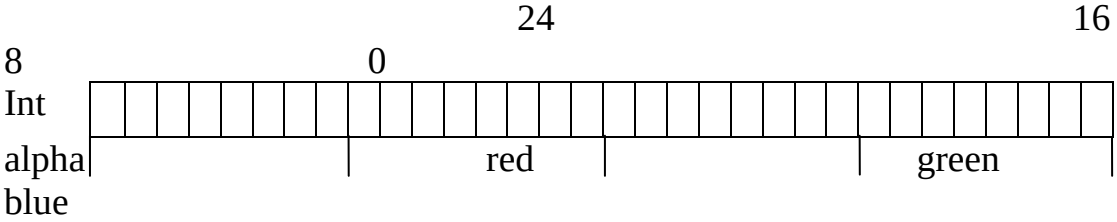

Figure (4) Red, Green, Blue and Alpha Values of Digital Image

7. General Algorithm of the Proposed System

This section illustrates the proposed general algorithm for approach. It is shown this in algorithm (1).

Input: Message (Plain text) **Output**: Cipher text hidden in Image
Process: **Step1**: Enter the text **Step2**: Encryption text using NTRU algorithm. **Step3**:The result from encryption operation is then embedded in the image using XOR method then Perform XOR operation on bits stored at part alpha location in pixel **Step4**: Save image after embedding the cipher text in image. **Step5**: send image over commination channel e.g. (viber ,yahoo mail or web site). **Step6**: The message receiver apply operation decryption of the message **Step7**: Extract the result from the image saved in embedding operation that the cipher text uses XOR operation and information hidden is executed from image. **Step8**: After extraction cipher text from image works decryption operation using NTRU algorithm. **Step7**: The result from decryption is plaintext **Step8**: End.

Algorithm (1) General Algorithm of Proposed Approach

8. Experimental Work

Each step in algorithm (1) will be described in the following example the main interface of the proposed system is content two part (Encryption & Hidden Information, Decryption) as show in figure (5).

Figure (5) the Main Interface of the Proposed System

Step1: Choice the Encryption& Hidden Information will appear interface that include NTRU algorithm as show in figure (6).

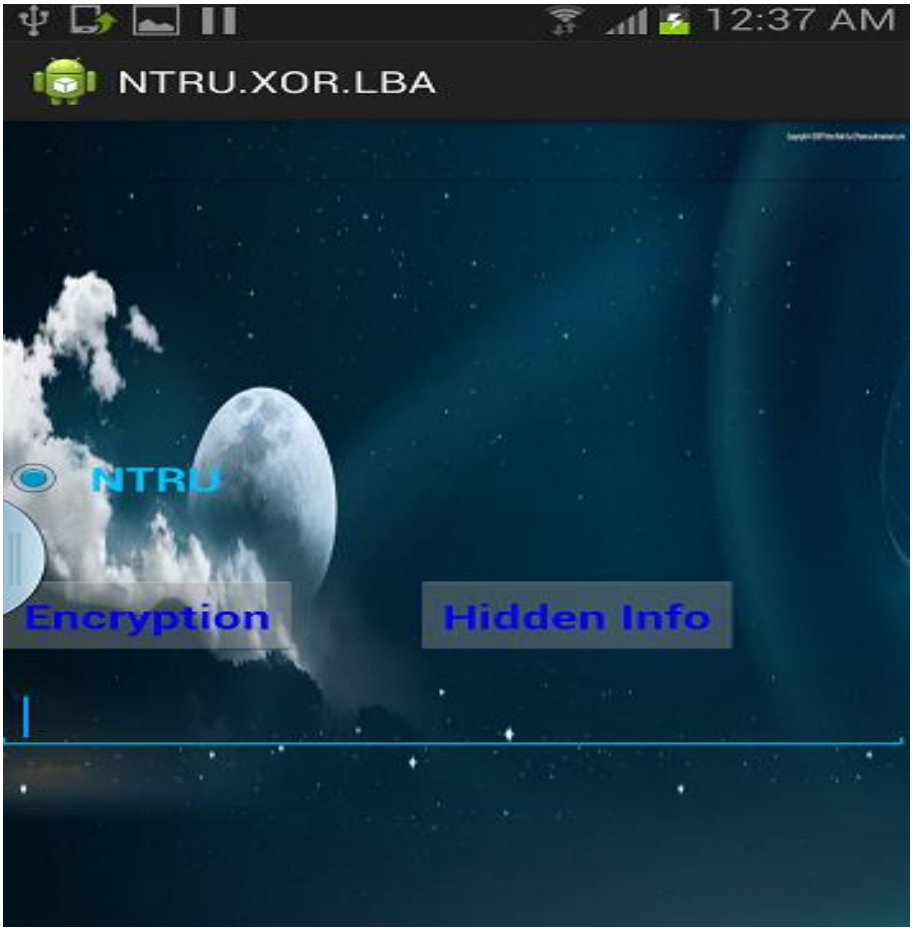

Figure (6)The Main Interface of Encryption & Hidden Information

Step 2: The message **"Faculty of Education at the University of Mustansiriya will evaluate scientific conference "**is entered using NTRU algorithm and the result from the result from encryption of massage is **"c2R58P<U@233OdAMELUU;9Mdha:DTFaLglnB78BCSSY85_HFCGJ5KTb=69Vb:2efK[d'F;ZOElgVePG515UGH:cPPX^KLRW\8@ad<feMAbXDed85QJ726>::Oc@QXN3Ol'DgaYM;'6|K_7Xb:FPg@l;4ZGAD'YK@g='>EG'g98[CDlN"**is Cipher text as Illustrated in Figure (7).shown in Figure (7).

Figure (7) Encryption of Message by Using NTRU Algorithm

Step 3: choice hide information to hide of massage that encrypted by NTRU Algorithm, then choice open picture Gallery then Hidden message by XOR Method than save picture, as illustrated in Figure (8).

Figure (8) Load the Image

Step 5: after access the message for receiver will make decryption the message by click on back to Home window, then open picture than upload to picture that hide of message than click on Extract info from picture, the result from Extract is, as illustrated in Figure (9).

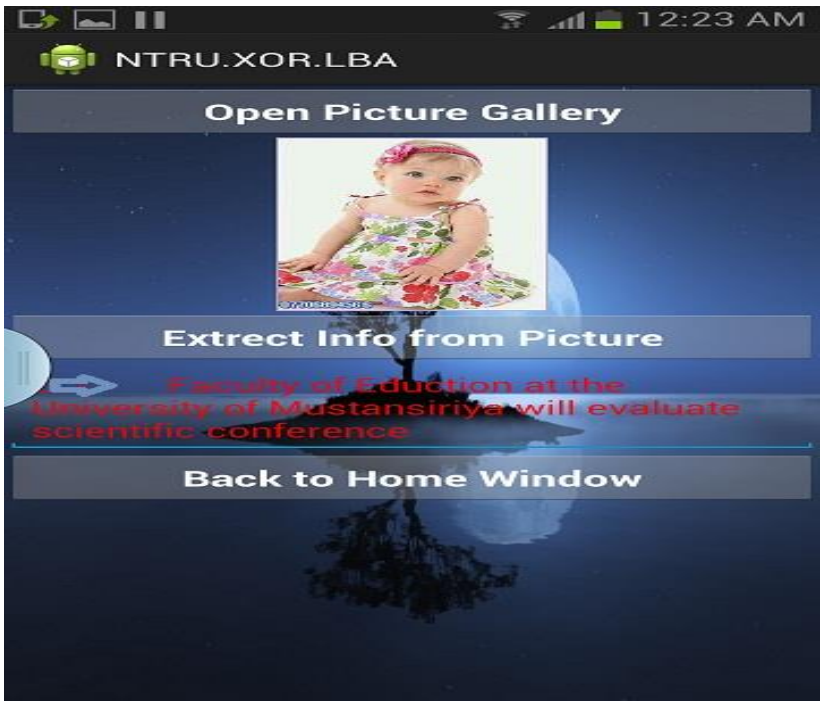

Figure (9) Decryption by using NTRU algorithm

Step 7: End.

9. Experiment Test to the Proposed System

This section illustrated the results that obtained from execute the proposed system and its testing results by using PSNR and MSE. The tests were applied to color images from format (BMP) for size (256*256) to select the highest (PSNR) value with its minimum value of (MSE). For all the experiments presented the following tables compares the maximum PSNR and minimum MSE of NTRU algorithm of the proposed system. As shown in the following figures (١٠) & (١١) the images before embedding text and the images after embedding text.

Figure (1 ing text

Figure (11) The images after embedding text

The result from test after apply encryption text by using NTRU algorithm and embedding text in the image are found the image cover child, Family and Lena are the best using The image format Bmp as shown in the table (1).

Table (1) Values of PSNR and MSE After Use Algorithm for BMP Images

	PSNR Value	MSE Value
Image Cover	NTRU	NTRU
Apple	59.1445	1.1148
Child	62.0242	0.7575
Family	55.1834	0.6586
Lena	61.7725	0.5635

10. Conclusions

1. This paper presents a method for encrypting messages of mobile in the android operating system environment using NTRU algorithm.
2. The NTRU algorithm is a public key cryptosystem which is very fast cryptosystem and it is based on rings. It gives advantages for easy generation of keys and high speed. The entire operations contained in these procedures are convolution multiplication, addition and modular arithmetic. NTRU cryptosystem appropriately, the analysis and description in this paper has vast importance.
3. This paper gives brief description and analysis of the NTRU Cryptosystem and provides some help in the improvement of the cryptosystems for the network security.
4. This proposed system can be used in all types of JAVA enabled mobile devices and compatible with any type of mobile phone and tablet devices that use Android operating system.
5. Hiding the text into the image using LSB technique with the help of XOR operation gives more security and complexity
6. The approach is compatible with any type of mobile phone that use Android operating system.
7. The execution of the approach in the mobile phone is faster and added another layer of security by using NTRU algorithm.

8. Use of steganography and cryptography together provides strong security and invisible communication and

9. From experimental results, it is seen that the proposed method is effective because the result for PSNR and MSE, and no difference is found between the original image and the stego image and when using NTRU algorithm.

References

[1] Min's, **Multimedia Data Hiding**, Ph. D.Thesis. Dissertation, Princeton University, April 2001.

[2] W. Bender, D. Gruhal, N. Morimoto and A.L.U. , **Techniques forData Hiding**, IBM System Journal, Vol. 35, No 3 &4, 1996.

[3] Richard Popa, "**An Analysis of Steganographic Techniques**" , Dept. of Computer Science and Software Engineering,Faculty of Automatics and Computer , University of Politehnica, Timisoara,1998.

[4] S.Inoue,K. Makino and O. Takizawa, "**A proposal on Information Hidind Methods using XML**", Yokohama National University.

<http://www.takizawa.ne.jp/nlp_xml.pdf>

[5] Samir Kumar Bandyopadhyay and Somaditya Roy, "**Information Security through Data Encryption and Data Hiding"**, International Journal of Computer Applications (0975 – 8887), Vol. 4, No.12, August 2010.

[6] SamerAtawneh," **A New Steganographic Algorithm for Hiding A Plain Text in Gray Images Using Blocks"**, Information Technology & National Security Conference, 2007.

[7] Roceanu I., "**Knowledge Anywhere, Anytime Based on the Wireless Devices**," in Proceedings of the 5th Scientific Conference eLearning and

Software for Education, Bucharest, pp. 68-72, 2009.

[8] Schiffman J., Zhang X., Gibbs S., Kunjithapa A., and Jeong S., "**Securing Elastic Applications on Mobile Devices for Cloud**

Computing," *in ACMCloud Computing Security Workshop*, USA, pp. 127-134, 2009.

signature scheme", Ph.D.Thesis, FomerlyAgera University, 2003.

[10] Piper F. and Murphy S., "**Cryptography: A very short introduction**", Oxford university press, 2002. http:// www.Books24×7.com/Refrenceware for professionals.htm.

[11] Wikipedia, **"Encryption",** http://en.wikipedia.org/wiki/Encryption, modified on 13

December 2006.

[12] Freeman J., Neely R., and Megalo L. **"Developing Secure Systems: Issues and**

Solutions".IEEE Journal of Computer and Communication. 1998.

[13] Coppersmith and A. Shamir, "**Lattice attacks on NTRU**," in Proc. of Euro crypt 97, Lecture Notes in Computer Science, Springer-Verlag, 1997[CS97].

[14] V. Sandhya, "**A Study on Various Security Methods in Cloud Computing**", International Journal of Advanced Research in Computer Science, Volume 2, No.6, Nov-Dec 2011.

[15] J. Hoffstein, D. Lieman, J. Silverman" **Polynomial Rings and Efficient Public Key**

Authentication", Proceeding of the International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99), M. Blum and C.H. Lee, eds., City University of Hong Kong Press,1999.

[16] Cox I. J., et al. "**Digital Watermarking and Steganography**", 2nd Edition, Morgan Kaufmann Publishers, Elsevier Inc.(2008)

[17]Shirali-Shahreza M. H. and Shirali-Shahreza M., "**A New Approach to Persian/Arabic Text Steganography**", 5th IEEE/ACIS International Conference on Computer and Information Science, 310-315. (2006)

[18] N. Cvejic, *Algorithms for Audio Watermarking and Steganography*. Finland: Oulu University Press, 2004.

[19] J. C. Judge, "**Steganography: Past, Present, Future**", *SANS white paper*, 2001. URL: http://www.sans.org/rr/papers/index.php?id=552, last visited: 31 March 2008.

[20] Ahmed Ch. Shakir," **Steno Encrypted Message in Any Language for Network Communication Using Quadratic Method**", Journal of Computer Science 6 (3): 320-322, 2010 ISSN 1549-3636 © 2010 Science Publications.

[21] Wang, H & Wang, S, **"Cyber warfare: Steganography vs. Steganalysis"**, *Communications of the ACM*, 47:10, October 2004.

[22] seddik,A. H.," **Enhancing the (MSLDIP) Image steganographicmethod (ESLDIP Method)** ", International Conference on Graphicand Image Processing (ICGIP 2011), Proc. of SPIE Vol. 8285, 82853I, © 2011 SPIE.

[23] Abdul-Sada, A. I., " **Hiding Data Using LSB - 3** ", J.Basrah Researches (Sciences), Vol. 33, No.4. (81-88), December, 2007.

[24] Swain, G. and Lenka, S. K., " **A Novel Approach to RGB Channel Based Image Steganography Technique** ", International Arab Journal of e -Technology, Vol. 2, No. 4, June 2012.

[25]Android.**"WhatisAndroid?"**http://developer.android.com/guide /basics/what-isandroid.html,retrieved March 4, 2010.