Encryption and Decryption of Images using GGH Algorithm: Proposed

* Qusay Kanaan Kadhim ¹, Basman M. Al-Nedawe ², Emad Majeed Hameed ³

¹, ², ³ Technical Institute Baqubah, Middle Technical University, Iraq
¹ Department of Computer Techniques Engineering, Bilad Al Rafidain University College, Baqubah, Iraq

* Email: qusay.knaan@mtu.edu.iq & qusaykn@gmail.com

Abstract. Images are considered as important data used in many fields such as military operations, medical imaging, and astronomy researches. For sending images through an insecure network, it is necessary to develop a secure encryption algorithm when transmitting the images. Three main properties of security services (i.e., confidentiality, integrity, and availability), the confidentiality is the most essential feature for exchanging images. The Goldreich Goldwasser Halevi (GGH) algorithm can be a good method for encrypting images as both the algorithm and sensitive data are represented in numeric matrices. Additionally, the GGH algorithm does not increase the size of the image. However, one of the disadvantages of using the GGH algorithm is the attacking of GGH cryptosystem mainly relied on special properties of the lattice generated. This shortcoming of GGH algorithm has been taken to proposed lattice reduction algorithms. A lattice basis reduction algorithm to get a better basis which is used into encryption and decryption approach.

1. Introduction

The cryptography is considered as one of the attractive topics and important in many technologies. When a user transfers any data between systems using a public network, those data must be protected using an encryption algorithm [1]. Encrypting an image means to apply a symmetric or asymmetric encryption algorithm to an input image to be converted into a cipher image using either symmetric or asymmetric keys [2]. Symmetric ciphers only use one key for encryption and decryption processes while asymmetric ciphers use two different key pairs (i.e., public and private keys) [5]. Through default, the digital image is represented in the form of (2D) matrix of elements [3]. Each element in the matrix is called a pixel, each pixel contains digital number. If the dimensions of the matrix are equal, then it is called the square matrix [4]. As digital image is a matrix, then it is possible to denote the pixel by means of its position (r, c), where (r) is the row and (c) is the column [5]. To encrypt any digital image, an encryption algorithm (asymmetric or symmetric) must be applied on the original image in order to convert it to a ciphered image [6]. In asymmetric algorithm, two different keys (public and private) are used in encryption and decryption. While the symmetric algorithm uses the same key (private) in encryption and decryption [7]. The strength of the algorithm of encryption or decryption comes from its ability to stand against the famous attacks [8]. Therefore, providing a strong and safe environment by the encryption algorithms is important for images and data [9].
The important factors which makes the GGH algorithm more suitable for image encryption are it is based on public key cryptosystem, it has a numerical matrix/lattice based scheme which is suitable for images, and it has the low computations cost and fastness properties [10]. Based on the architecture of the GGH encryption algorithm, the size of ciphered image will be the same as the original image, but the bit sizes of cipher image will be increased when being compared to the original image [11]. Most of the time, GGH produce errors in decrypted data which makes it inaccurate. This error exists only at the right LSB bits (least significant bits), so the pixel will not change a lot and lead to that the original image can be retrieved easily [12]. Finally, we proposed a strategy for strengthening the security of the GGH cryptosystem; a lattice basis reduction to the public key is to get a better basis, which is used to encryption and decryption.

2. Literature Review

2.1. Lattice
A lattice can be defined as a subgroup of \((\mathbb{R}^m)\). This subgroup must be discrete and additive [13]. Basically, an n-dimensional lattice \((\mathcal{L})\) consists of a set of points \((\mathcal{L} = \{b_1, b_2, ..., b_n \in \mathbb{R}^m\})\) [14]. These points are n-linearly independent vectors. The vectors represent the basis to generate the lattice \((\mathcal{L})\) which is also a vector defined in eq. (1) [15][16]. The Figure.1 illustrates the lattice in \((\mathbb{R}^2)\) [17].

\[
\mathcal{L} = \mathbb{Z} \langle b_1, b_2, ..., b_n \rangle = \{ \sum_{i=1}^{n} \alpha_i b_i | \alpha_i \in \mathbb{Z} \}
\]

\[\text{(1)}\]

Figure 1. A Lattice in R2

Figure 1. present the first lattice-based cryptography using the worst case problem (WCP) [18]. Another lattice-based cryptography (GGH) using the closest vector problem (CVP) was presented by Goldreich, Goldwasser, and Halevi [19]. The new cryptography depends on lattice and the shortest vector problem (SVP) [20]. The first lattice-based cryptography based on worst-case problem was presented by Ajatai and Dwork in 1997 [21]. After that, there have been a lot of improvements over lattice-based cryptography algorithms. In 1997, Goldreich, Goldwasser, and Halevi also presented a lattice-based cryptography based on closest vector problem (CVP) [22]. In 1998, Hoffstein and Silverman, presented a new lattice-based cryptography using the shortest vector problem (SVP) which works on polynomials [23].

2.2. GGH Algorithm
In this study, we have taken the advantage of the GGH algorithm for encrypting the images. The GGH cryptosystem is based on CVP which is one of the NP-hard problems presented in 1997 by Goldreich et [24]. It also introduces a trapdoor as an one-way function for implementing a public key cipher which
relies on difficulty of lattice reduction [25]. For increasing its own security feature, this algorithm uses a public key that depends on the strength of lattice for generating a trapdoor function [24]. To implement the encryption process, the message must be encoded as a lattice vector using the public basis, after that a small error vector must be added. While in implementation of the decryption process, the private basis must be used to compute the closest lattice vector in an efficient way [11]. The GGH is analogous to McEliece with some improvement. The encryption process is performed randomly. The security of GGH relies on the dimension of the lattice (n) and the security parameter (σ). The complexity of CVP is presented thru (σ) [26]. Altogether challenges of the security parameters were attacked by Nguyen when n=200, 250, 300, 350 and 400 except for n>400, because of the huge size of the key, and this makes the security to be in high levels [27]. The GGH uses the parameters illustrated in Table.1 [28].

| Parameter | Description | Knowledge |
|-----------|-------------|-----------|
| n         | Dimension   | Public    |
| σ         | Security Parameter | Public    |
| R         | n * n Integral Matrix | Private |
| B         | n * n Integral Matrix | Public    |

The matrices (R) and (B) represent the private key and the public key respectively. The matrix (R) include a good basis of the lattice (A) which is reducible, whereas the matrix (B) include a bad basis of the lattice (A) which is irreducible, such that (A ⊂ Z^n) and the basis includes the short vectors [25].

Several methods can be used to generate the private matrix (R), one of them is to select a random matrix that consists of short vectors. The other method is by using eq. 2 below:

\[ R = K \cdot I_n + E \]  

Where (K) is an integer whose size is medium and more than 1, (I_n) represent the n*n identity matrix and (E) represents a random matrix of short vectors. Also, several methods can be used to generate the public matrix (B) from the private matrix (R) randomly. One of these methods can be implemented by multiplying (R) by a random uni-modular matrix (U), such as in eq.(3 below [11])

\[ B = U \cdot R \]  

Suppose that (m), (e) and (c) represent the message, error and cipher matrices respectively, then to implement the encryption and decryption processes using GGH algorithm, it is important to use eq. 4, 5 and 6 as below:

- The encryption process:
  \[ c = m \cdot B + e \]  

- The decryption process:
  \[ \text{round (c. R-1)} = \text{round ((m. B + e). R-1)} = m \cdot U \cdot R \cdot R^{-1} + \text{round (e. R-1)} = m \cdot U + \text{round (e. R-1)} \]

The eq. 6 the value (e. R-1) is small so it can be removed by using the technique of Babai rounding [28].

2.3. Key Generation

The process of key generation, it is important to know a theory that is used in ElGamal cryptosystem for generating the key [29]. The theory is known as primitive root theory [30]. Theory assures that for any large prime number (p), there exists an integer number (α | 1 ≤ α ≤ p-1), such that all remainders (α^t (mod p) | 1 ≤ t ≤ p-1) are distinct. The integer number (α) is known as a primitive root modulo (p) [1].
After selecting \((p)\) and \((\alpha)\), a random parameter \((d \mid 1 < d < p - 2)\) must be computed. The three parameters \((p, \alpha, d)\) are used to compute \((\beta = a^d \mod p)\) [9].

The encryption key \((p, \alpha, \beta)\) is the public key that will be used to encrypt the message. It is important that the random number \((d)\) that is used to compute \((\beta)\) to be private to be used later in the decryption process [31].

2.4. Encryption

The suppose that Alice needs to send a message \((M)\) to Bob. The encryption process can be explained depending on the steps below that must be performed by Alice [32][29].

- Obtaining the public key \((p, \alpha, \beta)\) from Bob.
- Converting the message \((M)\) into a numerical representation as a set of integer numbers \(m_1, m_2, \ldots \mid 1 \leq m \leq p - 1\). These numbers will be encrypted one by one.
- Selecting a random integer number \((k)\), that must be secret.
- Computing the public key \((r = a^k \mod p)\).
- Encrypting the message \((M)\) to the ciphertext \((C)\), such that \((c_i = m_i \times \beta^k \mod p)\), where \((C)\) represents the set of every \((c_i \mid 0 < i \leq |M|)\).
- Sending the ciphertext \((C)\) to Bob together with the public key \((r)\).

2.5. Decryption

The perform the decryption process, Bob must use the ciphertext \((C)\) and the public key \((r = a^k \mod p)\). The decryption process depends on the steps below [33].

- Computing the shared key by combining the private number of Bob \((d)\) with the random number of Alice \((k)\), such that \(((a^k)^{p-1-d} = (a^k)^{-d})\).
- Decrypting the ciphertext \((C)\), such that \((m_i = (a^k)^{-d} \times c_i \mod p)\), where \((m_i)\) is the plaintext part corresponding to the ciphertext part \((c_i)\) [1].

The message \((M)\) that are sent by Alice can be read by Bob after combining all plaintext parts \((m_i)\) [30].

3. Approach GGH Algorithm

The mechanism of GGH algorithm, assume that there is a sender and receiver called \((A)\) and \((B)\) respectively.

\((B)\) must do these steps:

- Selecting an image and using it to generate his private key form eq. (2).
- Generating a uni-modular matrix in random way.
- Using eq. (3) to compute another image as a public key.
- Sending the image obtained from step (3) to \((A)\).

The other hand, \((A)\) must use eq. (4) for encrypting his 3D-image and sends to \((B)\). \((B)\) receives the encrypted image which has a noise and uses eq. (5) and (6) for decrypting the received image into the original image. Note that the matrices \((R)\) and \((B)\) of GGH algorithm must be 3-dimensional matrices, i.e. \((n \times n \times n)\).

4. Attacks on GGH

The first remarkable attack to the GGH cryptosystem comes from Phuong Nguyen [24] in 1999. The attack works by carefully choosing \(n\) linearly independent lattice points, then constructing a new basis to generate a sub lattice of the original lattice by those \(n\) points. Then we attack the sub lattice to identify the potential properties of the original lattice [26]. The dimension of GGH lattice should be larger than 250 guarantee the security [34]. It shows that the signature encrypted with the GGH cryptosystem is insecure in certain special situations. When the special situation occurs, the GGH signature is insecure.
even the dimension of the GGH is as large as 1000 [11]. Since the GGH cryptosystem relies on the orthogonality of the bases for a lattice. It turns out that the Lattice Reduction algorithms can produce nearly orthogonal bases based on the Public Key. Hence running Lattice Reduction algorithms on the Public Key will give us good bases that can be regarded as quasi private keys to attack the GGH cryptosystem to Lattice Reduction algorithms [22]. When we try to generate a new basis using lattice reduction algorithms, the quality of the new produced basis is mainly determined by two issues. Firstly, it depends on what lattice reduction algorithm it used. Secondly, this quality also highly relies on the approach of finding a shortest vector within the lattice reduction algorithm [11]. When plug different SVP solving algorithms to a lattice reduction algorithm, can achieve various reduced bases of different qualities for example, LLL reduction algorithm [35].

4.1. LLL Reduction Algorithm
The LLL algorithm [36] is one of the most important milestones on research of lattice reduction methods, although it was first proposed in order to factorize polynomials. The erotically, it runs in polynomial time where n is the dimension of a given lattice L and P is the maximal Euclidean Length of vectors in the given basis. It produces a reduced basis, whose shortest vector can be regarded as a solution of SVP [35]. Because of the high performance of the LLL algorithm in practice, it has become a fundamental tool in lattice reduction algorithms [37][36].

5. Conclusions
GGH is a simple public key crypto system which is based on the closest vector problem (CVP). It encrypts data in the matrix form and makes it suitable for image encryption. It works in different dimensions and different square matrices. The capability of encryption top secret information remains as a problem in the GGH encryption, which depends on various attacking methods. The early approaches to attacking the GGH encryption mainly relied on special properties of the lattice generated.so a method is proposed a lattice basis reduction algorithm is to the public key to get a better basis, which is used to encryption and decryption approach. In the proposed approach lattice reduction algorithms, the LLL algorithm. whose shortest vector can be regarded as a solution of SVP of the high performance of the LLL algorithm in lattice reduction algorithms. This approach takes advantage of lattice theory, number theory and lattice reduction algorithms. Further discovered more strategy for strengthening the security of the GGH cryptosystem by preventing any potential attacks. The future works Implementation a LLL algorithm analysis of complexities for the algorithm will be related to the dimension of the GGH Lengths of the vectors in the Public Key. procedure Basis Enumeration with other SVP solving algorithms to increase the performance of the lattice reduction algorithms in the future.

Reference
[1] O. A. Imran, S. F. Yousif, I. S. Hameed, W. N. Al-Din Abed, and A. T. Hammid, “Implementation of El-Gamal algorithm for speech signals encryption and decryption,” *Procedia Comput. Sci.*, vol. 167, no. Iccids 2019, pp. 1028–1037, 2020, doi: 10.1016/j.procs.2020.03.402.
[2] V. M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso, and M. Aldape-Pérez, “Substitution box generation using Chaos: An image encryption application,” *Appl. Math. Comput.*, vol. 332, pp. 123–135, 2018, doi: 10.1016/j.amc.2018.03.019.
[3] H. S. M. Alsultani, S. T. Ahmed, B. J. Khadhim, and Q. K. Kadhim, “The use of spatial relationships and object identification in image understanding,” *Int. J. Civ. Eng. Technol.*, vol. 9, no. 5, 2018.
[4] G. Kaur, R. Agarwal, and V. Patidar, “Chaos based multiple order optical transform for 2D image encryption,” *Eng. Sci. Technol. an Int. J.*, vol. 11, no. 3, 2020, doi: 10.1016/j.jestch.2020.02.007.
[5] Q. K. Kadhim, “Image compression using Discrete Cosine Transform method,” *Int. J. Comput. Sci. Mob. Comput.*, vol. 5, no. 9, pp. 186–192, 2016, [Online]. Available: www.ijcsmc.com.
[6] B. Arpacı, E. Kurt, and K. Çelik, “A new algorithm for the colored image encryption via the
modified Chua’s circuit,” *Eng. Sci. Technol. an Int. J.*, vol. 23, no. 3, pp. 595–604, 2020, doi: 10.1016/j.ajestch.2019.09.001.

[7] Z. Hua, Y. Zhou, and H. Huang, “Cosine-transform-based chaotic system for image encryption,” *Inf. Sci. (Ny)*, vol. 480, no. 30, pp. 403–419, 2019, doi: 10.1016/j.ins.2018.12.048.

[8] A. M. Elshamy, A. I. Hussein, H. F. A. Hamed, M. A. Abdelghany, and H. M. Kelash, “Color Image Encryption Technique Based on Chaos,” *Procedia Comput. Sci.*, vol. 163, pp. 49–53, 2019, doi: 10.1016/j.procs.2019.12.085.

[9] M. I. Fath Allah and M. M. Eid, “Chaos based 3D color image encryption,” *Ain Shams Eng. J.*, vol. 11, no. 1, pp. 67–75, 2020, doi: 10.1016/j.asej.2019.07.009.

[10] S. Zhu, C. Zhu, and W. Wang, “A new image encryption algorithm based on chaos and secure hash SHA-256,” *Entropy*, vol. 20, no. 9, 2018, doi: 10.3390/e20090716.

[11] S. Kamel, M. Sarkiss, and G. R. Othman, “Improving GGH Cryptosystem Using Generalized Low Density Lattices,” *IEEE Access*, pp. 1–6, 2016.

[12] S. A. Nie, G. Sulong, R. Ali, and A. Abel, “The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image,” *Int. J. Electr. Comput. Eng.*, vol. 9, no. 6, pp. 5218–5226, 2019, doi: 10.11591/ijece.v9i6.pp5218-5226.

[13] S. Rawal and S. Padhye, “Cryptanalysis of ID based Proxy-Blind signature scheme over lattice,” *ICT Express*, vol. 6, no. 1, pp. 20–22, 2020, doi: 10.1016/j.ictex.2019.05.001.

[14] M. Ge and R. Ye, “A novel image encryption scheme based on 3D bit matrix and chaotic map with Markov properties,” *Egypt. Informatics J.*, vol. 20, no. 1, pp. 45–54, 2019, doi: 10.1016/j.eij.2018.10.001.

[15] R. Chapaneri, T. Sarode, and S. Chapaneri, “Digital image encryption using improved chaotic map lattice,” *2013 Annu. IEEE India Conf. INDICON 2013*, no. December 2014, 2013, doi: 10.1109/INDICON.2013.6726031.

[16] X. Wang, N. Guan, H. Zhao, S. Wang, and Y. Zhang, “A new image encryption scheme based on coupling map lattices with mixed multi-chaos,” *Sci. Rep.*, vol. 10, no. 1, pp. 1–15, 2020, doi: 10.1038/s41598-020-66486-9.

[17] M. Abd et al., “A simple flexible cryptosystem for meshed 3D objects and images,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 7, pp. 1–18, 2019, doi: 10.1016/j.jksuci.2019.03.008.

[18] J. Huang, “applied sciences A Lattice-Based Group Authentication Scheme,” *Appl. Sci.*, vol. 8, no. 987, pp. 1–14, 2018, doi: 10.3390/app8060987.

[19] A. Mariano, T. Laarhoven, F. Correia, M. Rodrigues, and G. Falcao, “A Practical View of the State-of-the-Art of Lattice-Based Cryptanalysis,” *IEEE Access*, vol. 5, no. c, pp. 24184–24202, 2017, doi: 10.1109/ACCESS.2017.2748179.

[20] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, “The impact of quantum computing on present cryptography,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 405–414, 2018, doi: 10.14569/IJACSA.2018.090354.

[21] L. Liu, S. Wang, B. He, and D. Zhang, “A Keyword-Searchable ABE Scheme From Lattice in Cloud Storage Environment,” *IEEE Access*, vol. 7, pp. 109038–109053, 2019, doi: 10.1109/access.2019.2928455.

[22] P. Nguyen, “Cryptanalysis of the Goldreich – Goldwasser – Halevi Cryptosystem from Crypto,” *Springer-Verlag Berlin Heidelberg*, pp. 288–304, 1999.

[23] A. Sipasseuth, T. Plantard, and W. Susilo, “Enhancing Goldreich, Goldwasser and Halevi`s scheme with intersecting lattices,” *EJOURNALS*, vol. 13, no. 4, pp. 169–196, 2019.

[24] A. Mandangan, H. Kamarulhaili, and M. A. Asbullah, “A Security Upgrade on the GGH Lattice-based Cryptosystem,” *Sains Malaysiana*, vol. 49, no. 6, pp. 1471–1478, 2020, doi: 10.17576/sm-4906-
2020-4906-25.

[27] J. H. Cheon, J. Jeong, and C. Lee, “An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero,” J. Comput. Math., vol. 19, no. September 2016, pp. 255–266, 2016, doi: 10.1112/S1461157016000371.

[28] B. S. Massoud Sokouti, “THE GGH PUBLIC KEY CRYPTOSYSTEM VIA OCTONION ALGEBRA AND POLYNOMIAL RINGS,” Int. J. Inf. Technol. Secur., vol. 10, no. 4, pp. 77–86, 2018.

[29] F. Y. Rao, “On the Security of a Variant of ElGamal Encryption Scheme,” IEEE Trans. Dependable Secur. Comput., vol. 16, no. 4, pp. 725–728, 2019, doi: 10.1109/TDSC.2017.2707085.

[30] P. Mohit and G. P. Biswas, “Design of ElGamal PKC for encryption of large messages,” 2015 Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2015, no. July, pp. 699–703, 2015.

[31] A. M. Vengadapurvaja, G. Nisha, R. Aarthi, and N. Sasikaladevi, “An Efficient Homomorphic Medical Image Encryption Algorithm for Cloud Storage Security,” Procedia Comput. Sci., vol. 115, pp. 643–650, 2017, doi: 10.1016/j.procs.2017.09.150.

[32] A. Daeri, “ElGamal public-key encryption,” in International Conference on Control, Engineering & Information Technology (CEIT’14) Proceedings, 2014, pp. 115–117.

[33] W. D. M. G. M. Dissanayake, “An Improvement of the Basic El-Gamal Public Key Cryptosystem,” Int. J. Comput. Appl. Technol. Res., vol. 7, no. 2, pp. 40–44, 2018, doi: 10.7753/ijcatr0702.1002.

[34] K. Bagheri, M. R. Sadeghi, and T. Eghlidos, “An efficient public key encryption scheme based on QC-MDPC lattices,” IEEE Access, vol. 5, pp. 25527–25541, 2017, doi: 10.1109/ACCESS.2017.2765538.

[35] D. Ding, G. Zhu, and X. Wang, “A genetic algorithm for searching the shortest lattice vector of SVP challenge,” GECCO 2015 - Proc. 2015 Genet. Evol. Comput. Conf., no. September, pp. 823–830, 2015, doi: 10.1145/2739480.2754639.

[36] P. Xu, “Experimental quality evaluation of lattice basis reduction methods for decorrelating low-dimensional integer least squares problems,” EURASIP J. Adv. Signal Process., vol. 2013, no. 1, pp. 1–29, 2013, doi: 10.1186/1687-6180-2013-137.

[37] M. Fischlin and J. S. Coron, “Practical, Predictable Lattice Basis Reduction,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9665, pp. V–VI, 2016, doi: 10.1007/978-3-662-49890-3.

[38] D. Micciancio and M. Walter, “Practical, predictable lattice basis reduction,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9665, pp. 820–849, 2016, doi: 10.1007/978-3-662-49890-3_31.