Indian Journal of Science and Technology, *Vol 8(15), 70915, July 2015*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Bit Level Key Agreement & Exchange Protocol for Digital Image Steganography

N.D. Jambhekar[1*] and C.A. Dhawale[2]

[1]Department of Computer Science, S.S.S.K.R. Innani Mahavidyalaya, Karanja (Lad), District Washim – 444105, Maharashtra, India; ndjambhekar@rediffmail.com
[2]MCA Department, P.R. Pote College of Engineering & Management, Amravati, Maharashtra, India; cadhawale@rediffmail.com

Abstract

Background/Objectives: Key agreement and exchange process plays a critical role in information security. The existing steganographic key handling techniques use a symmetric key feature, where a single key is used by both parties for information concealing for security. **Methods/Statistical analysis:** This paper introduces a bit level key agreement and secured key exchange protocol for the digital image steganographic applications. This protocol is constructed with the help of simple binary arithmetic and the XOR operation, mostly suitable for digital image steganographic algorithms. The key exchange is supported by the trusted third party image database. The image database is a collection of different small size images suitable for low processing and small memory mobile computing system. **Findings:** The present research offers a secure way to exchange the steganographic keys between both parties engaged in the information security. With the help of this technique, the secret key needs not transfer from one end to another for information hiding and uncovering from the cover object. The method discussed in this paper requires a very short key size as compared to other methods. The key transmission process is secure along with the less processing time require to generate the keys. The key generation is carried out by the LSB insertion technique with the partial secret of each party engaged in the security data transfer. The key exchange protocol of this method is secure against the different types active and passive attacks. The secret key requirement is not dependent on the concealing side; besides, the key is directly available to the revealing side with the help of trusted third party with small binary computation. So the secret key becomes safe and undisclosed from the intruders. **Application:** This technique is flexible, confidential and beneficial for the variety of the steganographic data security techniques. It is suitable for low bandwidth wireless system and mobile computing applications, where the key transmission insecure because of the vulnerable communication network.

Keywords: Binary Arithmetic, LSB Insertion, Key Agreement, Key Exchange, Steganography

1. Introduction

Steganography contributes a lot to secure the data flows over the communication networks. Today, the images are extensively used in data communication all over the world. Images can be treated as a confidential data and need securely transfer between two parties. Steganography is a way to secure the data transferred over the communication networks[8]. The data may be any text, image or the multimedia contents, secured during the transmission with the help of various steganographic algorithms. The security is implemented by hiding the confidential information in another cover object, for example; text or image is hidden in another image.

The steganographic algorithms such as Least Significant Bit (LSB) insertion, Discrete Cosine Transformation (DWT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT) are good enough to secure the data[18,19.] Algorithms can require a key to encrypt and decrypt the data. In the absence of valid key, the decryption is not possible. The use of wrong key cannot yield the output or even produces the wrongoutput.

Figure 1 depicts the key agreement and exchange in

* *Author for correspondence*

the form of public key and private key. The asymmetric key algorithms such as RSA and others use the public key technique[1]. The symmetric algorithms such as DES, TDES and AES use the secret key technique. The key agreement and exchange is also required for the steganographic algorithms and can be handled by the secret key technique like the symmetric key cryptographic algorithms.

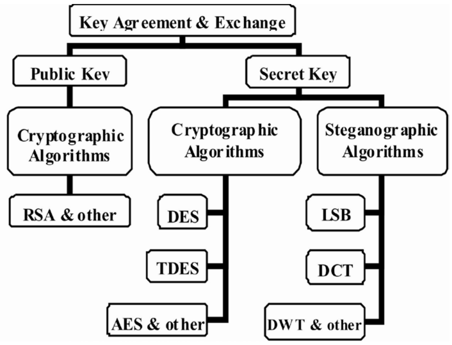

Figure 1. Key Mechanism of Security Algorithms.

The public key technique provides the facility to use one key for encryption and other key for decryption. Using the secret key technique, the same key is used for encryption and decryption[11]. This key must be kept securely by both the parties engaged in the communication. The Key is a string of symbols used during encryption and decryption. The security of algorithm breaks only in two conditions such as the weak key used with weak algorithmic structure and disclose of the private key.

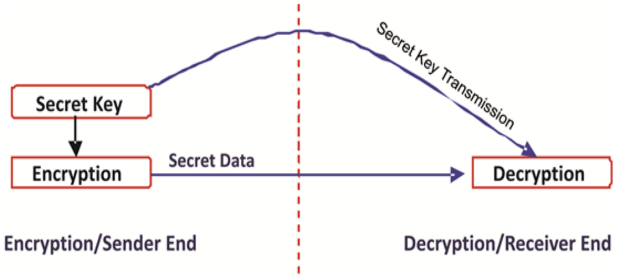

Figure 2. Secret Key Encryption/Decryption Technique.

Figure 2 shows the typical steganographic security mechanism used with the secret key technique. However, these mediums of key transmission can be accessed by the eavesdropper, who can easily access the confidential information using the stolen key. Therefore, the secret key exchange is vulnerable and the security is worthless even if the use of the stronger steganographic algorithm. To secure the key before transmitted to the other end, the key must be encrypted[20]. In this paper, we proposed a framework that gives a secure bit level key agreement and exchange protocol.

2. Key Selection

To secure confidential digital data transmitted over the data communication network, the security algorithms can use either Public Key or Secret Key technique[16]. The asymmetric algorithms such as RSA are solely using public key techniques where the Secret Key technique is used by the symmetric key algorithms. Steganographic algorithms require a key for encryption and decryption to increase the security while transmitting messages over the insecure communication network[5]. The steganographic algorithms use secret keys for the message security[9]. The key selection is a critical issue for the information security. The security key is classified not with the size of the key, but it must be secure against the potential attacks while transmitting it from one party to another. The key agreement[13] and exchange is secure enough to preserve the information security.

Some methods were used in the past recent years such as One Time Pad (OTP), DH key exchange and agreement protocol. These algorithms are attractive for their efficiency and function and are used in many security applications today. These algorithms are discussed below.

One Time Pad (OTP) cipher encrypts the message using the key as long as the size of the message to be encrypted, for example, if the confidential message is 1 megabyte; the key size must be 1 megabyte. If the key is shorter, it can be used multiple times[1]. The encrypted message and the large key used for encryption are then transmitted to another party. Due to the large key size, it is substantially difficult and time consuming during transmission. The small with repeating key is the solution, but it can break with some efforts[10].

In 1976, Diffie and Hellman facilitate two parties to share secrets and agree upon a common secret shared method by means of Diffie-Hellman key exchange and agreement protocol[12]. Because of this protocol, one party can communicate with the other party even if they are unknown to each other. In this protocol or an algorithm, both sender and receiver have their own public and private keys[17]. The public keys are derived from the private keys so that, public keys are openly available to anyone and private key is hidden by each party. If sender willing to send confidential information, it can use the receivers public key. This public key is used for encryption and decryption algorithm. The encryption algorithm can be any cryptographic algorithm and the receiver for decryption will use the same. The secret key is a product of a secret number selected by each party and other secret common number agreed by both. The third party can secretly provide this common number. Suppose two parties engaged in communication will be A and B. The steps for DH key generation are-

- **A** and **B** agree on a prime number ***p*** and ***g***
- **A** choose a secret integer ***sa*** and computes public key $pka = g^{sa} \bmod p$
- **B** choose a secret integer ***sb*** and computes public key $pkb = g^{sb} \bmod p$
- **A** compute $a = pkb^{sa} \bmod p$
- **B** compute $b = pka^{sb} \bmod p$

The DH protocol uses two prime numbers. The ***p*** is a large prime number and ***g*** is an integer number smaller than ***p***. The numbers are secret numbers and both **A** and **B** are agreed upon these. Here ***sa*** and ***sb*** are the secret numbers selected by themselves by the two parties **A** and **B** respectively. The ***pka*** is a public key of **A** and ***pkb*** is a public key of **B** computed from the secret keys ***sa*** & ***sb*** of **A** & **B** respectively. The public computation is shown in step 2 and 3. Because of the public keys of **A** & **B**, each party generates a secret code for the encryption by computing the public key of another party with self private key. The secret codes become ***a*** and ***b*** for party **A** and **B.** Party **A** computes the secret code ***a*** and encrypt the confidential data. Party **B** generates the secret code ***b*** and decrypts the encrypted message sent by the party **A.**

DH algorithm is widely used in various cryptographic algorithms and applications. This paper proposed algorithm for key generation and agreement, which is based on simple binary arithmetic used for the various steganographic operations such as Least Significant Bit (LSB) insertion.

3. Proposed Method

The Digital image is the sequence of pixels represented by the binary language well. Steganography is a way through which one digital object securely hidden in another object by means of various algorithms available such as Least Significant Bit insertion (LSB) algorithm[2]. This paper proposed the key agreement and exchange protocol suitable for the binary operations. The security of confidential information retains only if the key used for the encryption keeps secretly. While using the LSB insertion method, the key used for encryption must send to the receiver for decryption[14]. The key exchange is carried out by means of electronic transfer such as electronic mail as well as the physical transfer such as courier. The key generation process is carried out with the help of binary operations such as XOR. The XOR operation is shown using the following table.

Table 1. Simple Binary arithmetic using Bitwise XOR operation

A	B	Y=A xor B
0	0	0
0	1	1
1	0	1
1	1	0

XOR refers to the bitwise operator Exclusive OR. While two bytes are bitwise XOR produces another byte. For example

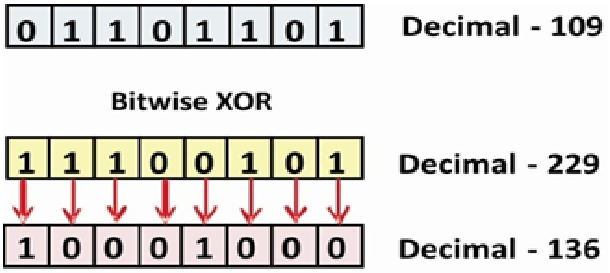

Figure 3. Simple Binary arithmetic using Bitwise XOR operation.

3.1 Key Agreement

The key agreement protocol of this algorithm facilitates two users to agree upon a shared secret binary number. This secret shared number gets processed with a secret key produces the public key. Both encryption and decryption end must agree upon a third party secret shared binary code. This can resolve the problem of transmission of encryption and decryption key via electronic or paper form. The public key generation in binary form is performed using little binary operations is stated using the following steps.

- Both encryption and decryption end must agree upon a common binary number used to generate their own public key.
- This common secret number can be available through a trusted third party.
- Both ends must select their private key in the form of binary bits.
- Each end generates their own public key using computing their private key with the shared secret number.
- The encryption side uses the decryption side's public key binary number to generate the partial encryption key.
- This newly generated partial secret key is then merged with third party provided image key, produces a complete stego key.
- This stego key is then used as the encryption key for steganographic algorithms.
- At the decryption end, the encryption side's public key is processed by the common secret number provided by the third party that generates the partial decryption key.
- At this end, the stego key generation is carried out using merging partial decryption key with the image key provided by trusted third party, which is identical with encryption end.

The public key generation using common secret number is shown below.

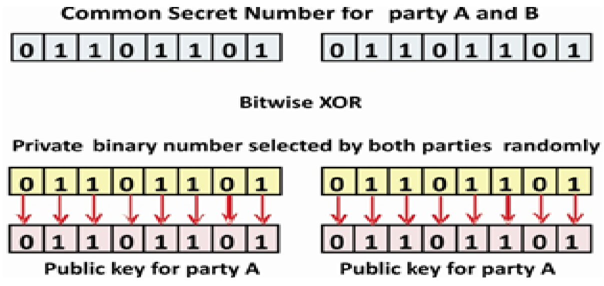

Figure 4. Public Key generation process using Bitwise XOR

The process of partial encryption and decryption key generation is given below

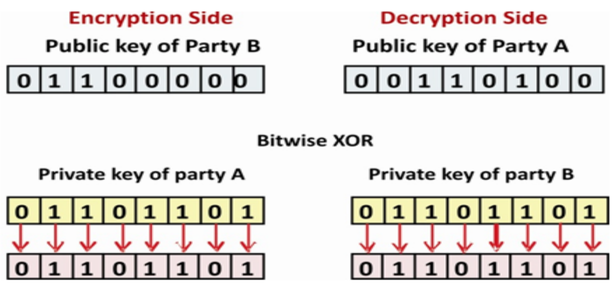

Figure 5. Partial Encryption/Decryption Keys generation process using Bitwise XOR.

Party A bitwise XORed the public key of Party B with its own private key while Party B bitwise XORed the public key of Party A with its own private key. The newly generate product at each end is the partial encryption and decryption key respectively.

3.2 Key Exchange

The key exchange part of this method is attractive due to the use of the third party in the process of the final key generation. A third party provides the image data to both encryption and decryption end. Due to the third party provided image, the final key can be strong enough with the help of public keys of both encryption/decryption ends.

The main objective of security enhancement is to use the image database provided by trusted third party. This image database resides on the trusted third party server or it may be available to both encryption and decryption end simultaneously. The selection of an image depends on the secret code shared by both parties. This secret image from the image database can be randomly selected and same for both the ends. This image database contains approximately 10000 images of size 3 megabytes only. Each image size is near about 300 bytes. These images are different from each other.

Whenever the partial key generated by the encryption and decryption end, one image from the third party provided image database, is selected and merged to generate the final stego key. This stego key is used for encryption and decryption. This operation is highly secret and no eavesdropper can break or predict the selection process of public key, image selection from image database and the formation of final stego key. The process is stated below.

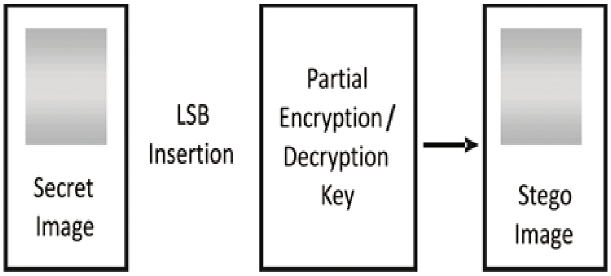

Figure 6. Final Stego Key generation using LSB insertion.

The stego key generation process is carried out by the LSB insertion[15] of binary form partial encryption and decryption key in one of the selected secret images from an image database. This stego key is then used for as secret key for steganographic algorithms for encryption and decryption. The newly generated stego key is dynamic and secure enough that no one can break the security mechanism of encryption/decryption system.

4. Performance Analysis

The effectiveness of the key generation, agreement and the exchange method is depends on the parameters such as key size, key transmission, processing time required to generate keys, speed to transfer encryption key to decryption size, flexibility, confidentiality of key during transmission and usefulness of the key method for different technologies. The comparative analysis of the OTP, DH protocol and the proposed method is discussed with respect of these parameters in the Table 2.

4.1 Key Size

Longer key size does not guarantee the security of confidential data. Shorter keys can be effective to provide the information security, but their proper framework must be implemented for the information security algorithm. One Time Pad (OTP) needs key size as long as the size of the secret message[3.] If the key is smaller, then it must be replicated to reach the size of secret message. DH protocol uses large prime number to generate the key. But in case of this proposed method the key can be very smaller and can be only eight bit code. Therefore, this proposed method is more attractive.

4.2 Key Transmission

Key transmission is a very crucial factor for every information security algorithm. If an unauthorized person discovers the encryption key, then the secrets can be easily uncovered. One Time Pad (OTP) requires its key to physically transfer to the decryption end with the help of paper mail or through electronic means such as email[4]. In case DH and the proposed method discussed in this paper, both need not transfer their secret keys. Therefore, DH and the proposed methods are beneficial over OTP.

4.3 Key Generation Time & Processing Time

One Time Pad (OTP) requires large processing time due to the use of large key. The DH protocol requires extra key generation time due to the large prime number used for the public key and private key generation. The proposed method discussed in this paper need the smaller size shared secret code of size eight bits only. Therefore, the key generation time required using this method is very small. The key processing time for both DH and the proposed method is less because these methods use the public key and private key features. Hence, the proposed method is beneficial over OTP and DH method.

4.4 Key Transmission Speed

One Time Pad (OTP) requires large transmission time and speed to transfer the encryption key towards decryption end because of the large key size. In case of DH and the proposed method, the keys need not transferred from end to end. Public keys are accessed by both the ends available in an open manner. Therefore, both methods are beneficial over OTP.

4.5 Flexibility

OTP supports the cryptographic methods, but cannot support the steganographic methods. DH protocol is well known for cryptographic method such as RSA but it cannot support the steganographic methods well. The proposed method described in this paper is flexible and can be used for the cryptographic as well as steganographic methods because of its bit-by-bit working fashion. It can effectively work and supports the steganographic methods such as LSB insertion. Hence, the proposed method is more flexible than the OTP and the DH protocol.

4.6 Confidentiality

Confidentiality plays a vital role in the security mechanism of any information security algorithm. During the transmission of key from encryption end to decryption

Table 2. Performance Analysis

Features	One Time Pad (OTP)	Diffie-Hellman Protocol	Proposed Method
Key Size	Same size of Secret Text or can be small	Large prime numbers used as secret shared code	Eight bits (1 byte) secret shared bit level code
Key Transmission	Electronic or physical transmission	No need to transfer keys due to public/private key form	No need to transfer keys due to public/private key form
Key Production Processing Time	Need large processing time due to large key	Need extra processing time due to large prime numbers used for secret shared code	Less processing time due to small eight bit code used as secret shared code
Key Transmission Speed	Need large communication speed due to large key transmission for decryption	Need very less communication speed because of small key size	Need very less communication speed because of small key size even for bigger data.
Flexibility	Not flexible to use in both Cryptographic and Steganographic methods	Suitable for Cryptographic methods, but not suitable for digital image steganographic methods	Suitable for Cryptographic methods and the steganographic methods due to bit level structure
Confidentiality	Breaks if key leaks during transmission	Strong Confidentiality	Strong Confidentiality
Usefulness	Useful in small amount of secret data	Useful in Cryptographic methods with no limit of data size	Useful in Cryptographic & steganographic methods with no limit of data size

end, the OTP method is not attractive and the security can be broken by discovering the key during transmission. The DH protocol and the proposed method discussed in this paper are highly secure and confidential, because the encryption/decryption key cannot be transferred physically or over the network electronically.

4.7 Usability

OTP is attractive for small amount of secret data. If secret data size increases, the key size also increases. In case of DH protocol, the size of the key is not depending on the secret data size. But it cannot useful for the steganographic methods. The method proposed in this paper is useful for both cryptographic and steganographic algorithms. The key size does not depend on the size of the secret data. Therefore, the proposed method is more attractive than the OTP and the DH protocol.

5. Conclusion

The secret key transmission system used by the existing steganographic algorithms can be easily known to the eavesdroppers because of the way the key transmitted. The proposed method efficiently solves this problem of secret key communication by providing the mechanism of a secret key and public key with the enhanced feature of partial key image selected from the third party supported secret image database. This bit level key agreement and exchange protocol are effective for the cryptographic and steganographic algorithms. In this paper, the performance analysis is carried out by analyzing some features with respect to the OTP, DH protocol and the proposed method. The proposed bit level key agreement and exchange method is more attractive in terms of a small key size structure, a safe key transmission system with only partial key transmission, less processing time for key production, required less transmission speed of key, flexible for any cryptographic as well as the steganographic based security system.

6. References

1. Stallings W. Cryptography and network security: principles and practice. 5th ed. India: Pearson Education; 2011.
2. Swain G. Digital image steganography using nine-pixel differencing and modified lsb substitution. Indian Journal of Science and Technology. 2014 Sep; 7(9):1444–50.
3. Borowski M, Lesniewicz M. Modern usage of “old” one-time pad. Military Communications and Information Systems Conference (MCC); 2012 Oct. p. 1–5.
4. Matt C, Maurer U. The one-time pad revisited. IEEE International Symposium on Information Theory (ISIT); 2013 Jul. p. 2706–10.
5. Dragan A F. Another steganographic LSB-based function. 9th International Conference on Communications (COMM); 2012 Jun. p. 311–14.
6. Schaefer RF, Khisti A. Secure broadcasting of a common

message with independent secret keys. 48th Annual Conference on Information Sciences and Systems (CISS); 2014 Mar. p. 1–6.

7. Liu X, Liu J, Chang G. A Four-Party password-based authentication key exchange protocol. 6th International Conference on Genetic and Evolutionary Computing (ICGEC); 2012 Aug. p. 280–3.
8. Kaur S, Bansal S, Bansal RK. Steganography and classification of image steganography techniques. International Conference on Computing for Sustainable Global Development (INDIACom); 2014 Mar. p. 870–5.
9. Dagadita MA, Slusanschi EI, Dobre R. Data hiding using steganography. IEEE 12th International Symposium on Parallel and Distributed Computing (ISPDC); 2013 Jun. p. 159–66.
10. Shukla R, Prakash H O, Bhushan RP, Venkataraman S, Varadan G. Sampurna suraksha: unconditionally secure authenticated one time pad cryptosystem. International Conference on Machine Intelligence and Research Advancement (ICMIRA); 2013 Dec. p. 174–8.
11. Liu S, Hong Y, Viterbo E. Unshared secret key cryptography. IEEE Transactions on Wireless Communications. 2014 Dec; 13(12):6670–83.
12. Li N. Research on diffie-hellman key exchange protocol. 2nd International Conference on Computer Engineering and Technology (ICCET); 2010 Apr. p. 634–7.
13. Anjaneyulu1 GSGN, Sanyasirao A. Distributed group key management protocol over non-commutative division semirings. Indian Journal of Science and Technology. 2014 Jun; 7(6):871–6.
14. Zielinska E, Mazurczyk W, Szczypiorski K. Trends in Steganography. Communications of the ACM. 2014 Mar; 57(3):86–95.
15. Rameshkumar P. Monisha M. Santhi B. Enhancement of information hiding in audio signals with efficient lsb based methods. Indian Journal of Science and Technology. 2014 Apr; 7(S4):80–5.
16. Barker E, Barker W, Burr W, Polk W, Smid M. Recommendation for Key Management - Part 1: General (Revision 3). Gaithersburg: NIST Special Publication 800-57, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology; 2012 Jul.
17. Mishra M, Tiwari G, Yadav AK. Secret Communication using public key steganography. IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014); 2014 May. p. 1–5.
18. Verma N. Review of steganographic techniques. International Conference and Workshop on Emerging Trends in Technology (ICWET–TCET); 2011 Feb. p. 990–3.
19. Srinivasan B, Arunkumar S, Rajesh K. A Novel Approach for Color Image, Steganography Using NUBASI and Randomized, Secret Sharing Algorithm. Indian Journal of Science and Technology. 2015 Apr; 8(S7):228–35.
20. Khan AS, Fisal N, Bakar ZA, Salawu N, Maqbool W, Ullah R, Safdar H. Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks. Indian Journal of Science and Technology. 2014 Mar; 7(3):282–95.