Diffie-Hellman Key Exchange through Steganographied Images

Submitted: 03/01/2018
Revised: 14/03/2018
Accepted: 18/03/2018

Amine Khaldi*

Abstract

Purpose – In a private key system, the major problem is the exchange of the key between the two parties. Diffie and Hellman have set up a way to share the key. However, this technique is not protected against a man-in-the-middle attack as the settings are not authenticated. The Diffie-Hellman key exchange requires the use of digital signature or creating a secure channel for data exchanging to avoid the man-in-the-middle attack.

Methodology/approach/design – We present a Diffie-Hellman key exchange implementation using steganographied images. Using steganography made invisible the data exchange to a potential attacker. So, we will not need a digital signature or creating a secure channel to do our key exchange since only the two concerned parts are aware of this exchange.

Findings – We generate a symmetric 128-bit key between two users without use of digital signature or secure channel. However, it works only on bitmap images, heavy images and sensitive to compression.

Keywords: Diffie-Hellman key exchange, key generation, symmetric key, data hiding, secret communication.

Introduction

The problem of secret data exchange had always existed, and cryptography offers an effective way to protect secret data by making it unintelligible to unauthorized persons, however, communicate with encrypted messages attracts attention (Bresson & al, 2007). This can be problematic when it comes to a communication channel monitored by a third party, which may at least suspicion, destroy communication between both parties. In this case, a communication containing a secret message between two persons must seem normal to the person who controls the channel. For this type of communication, steganography is the alternative solution to cryptography (Singh & Chawla, 2014).

*He is an Assistant Professor at the Université Kasdi Merbah of Ouargla (Faculty of New Technologies of Information and Communication) and has a Ph.D. in Image Processing and Steganography. His research area includes cryptography and steganography. Email: amine.vision@live.fr.

KHALDI, A. *Diffie-Hellman Key Exchange through Steganographied Images*. **The Law, State and Telecommunications Review**, Brasilia, v. 10, n. 1, p. 147-160, May 2018. [DOI: https://doi.org/10.26512/lstr.v10i1.21504]

Steganography is the art of concealing information. It hides a message in another innocuous message, so that we ignore the existence of the secret. While cryptography is based on the fact that the message is not understood, steganography is based on the fact that the message is not found. With the development of computers and networks, steganography has become a virtually unstoppable way to communicate secret information (Sumathi & al, 2013).

Our objective in this work is to implement a Diffie-Hellman key exchange using steganographied images to generate a symmetric key between two users; steganographied images will avoid us to use a secure channel to perform the exchange or digital signature for user's authentication. The data will be hidden so the exchange will be done secretly and discreetly without attracting the attention of a potential attacker.

The remainder of the paper is organized as follows: In section 2 we present an overview of the steganography process, its characteristics and its field of use. In Section 3, we will present the Diffie-Hellman key exchange algorithm. The application of the Diffie-Hellman key exchange through steganographied images is presented in section 4, and finally, conclusions from the work are drawn and further research work is suggested.

Steganography

Definition

Steganography is the art of information hiding (Siper & al, 2005). Unlike cryptography, steganography does not aim to secure a communication, but to hide its existence « Figure.1 ». In some situations, transmit encrypted data will be deemed suspect. Actually, more and more countries are developing strong restriction on the length of cryptographic keys and cryptography in itself. The renewed current interest for steganography comes from these restrictions on cryptography. Generally, steganography arrives in strengthening to the data encryption. To ensure maximum confidentiality, data is first encrypted before it is hidden using a steganographic process. Steganography therefore aims to maintain a secure communication without attracting the attention.

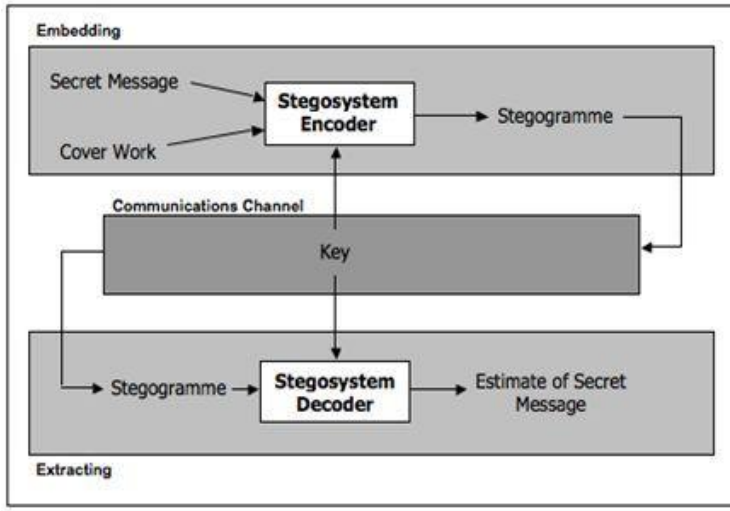

Figure 1 – Steganography process

Use of steganography

Previously, the messages were written on the shaved head of a slave. Once her hair was pushed, he could convey the message without being worried. Other well-known methods have emerged thereafter. Thus, invisible ink had great success in the last few decades. The idea was to write the message to remain secret invisible ink (lemon juice) and then write a clearly visible ink message to innocuous content (Mstafa & Bach, 2005). At destination, special treatment allowed to recover the message.

Currently, steganography is applied to digital media (audio, video or image) it represents the ideal media for transmitting information. With the spread of the Internet, the volume of data it represents is very important. The attacks of September 11, 2001 have revived the interest of academic and professional for steganography. The use of steganographic techniques for organizing these misdeeds would be the main factor.

Steganography protocols

There are three types of steganography protocols, closely matching that exist in cryptography.

- Pure steganography (Sharma, 2015) is a system in which the data concealing secret lies only in the algorithm used for this purpose«

Figure.2 ». The discovery of this algorithm breaks the concealment of communication.

Figure 2 – Pure steganography process

- Secret key steganography (Dagar & al, 2013) is similar to symmetric cryptography, the exchange of confidential data requires, first, the exchange of a secret key and it is therefore necessary to have a secure channel, or meet in person our interlocutor, to be sure that the key is not compromised. This key is used during the steganography process« Figure.3 ».

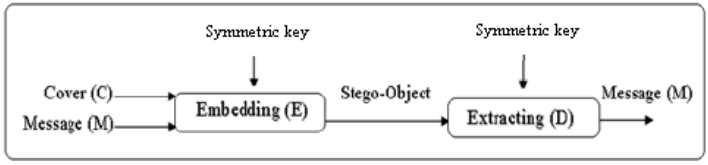

Figure 3 – Secret key steganography process

- Public key steganography (Takebe & Tanaka, 2013) is similar to the asymmetric cryptography. The person, who wants to send data to another party, without arousing suspicion, will use the public key of this person« Figure.4 ». The public key is known to everyone, there will be no need for prior exchange. The person receiving this message will be the only one able to extract its content using its private key.

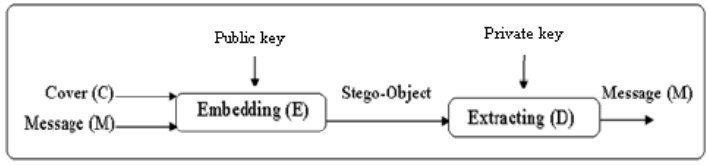

Figure 4 – Public key steganography process

Characteristics

Three criteria (Dittmann; 2006) are used to classify the steganographic algorithms: The capacity, transparency and robustness « Figure.5 ». These three requirements cannot be maximized simultaneously. Each will influence the other.

- The capacity corresponds to the mass of data which can be inserted in a container, in relation to its size.
- Transparency quantifying the noise generated by the concealment process and the invisibility of our message.
- Finally, the robustness specifies the capacity of our message to remain intact if the container is changed (Filtering, compression).

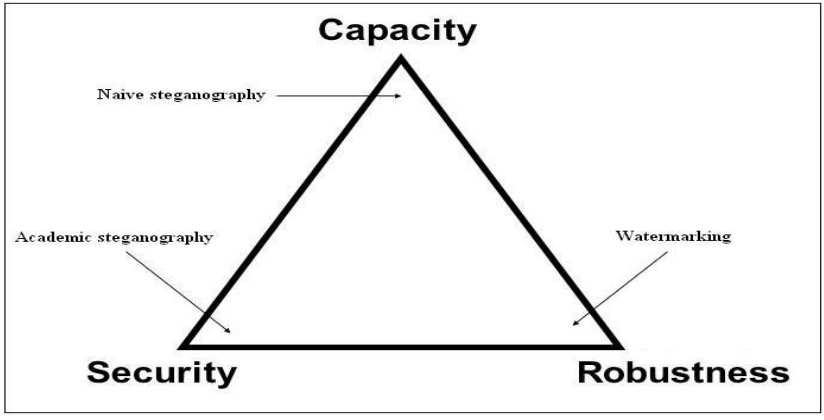

Figure 5 – Steganography characteristics

Steganographic tools

- The tools of naive said steganography correspond to the majority of tools available online. They hide the information in the containers without really worrying about the ease of detecting the data or the influences that these data can have on the container from a statistical point of view.
- Academic steganography tools are developed by research teams. Their goal is to evolve in parallel with steganalysis technics. Their main objective is to achieve fully transparent algorithms (for current methods). Recent research focuses on maximizing the available space concealment.

- Finally, the watermarking tools, mainly used for copyright protection, are mainly developed to have a high robustness. Unlike steganography, their opponents are the active type. The contents of watermarking do not interest them, their objective is to remove it.

Steganography domain

Steganography is divided into two areas, spatial and frequency domain. In the special domain, the secret message is inserted into the pixels of the image while in the frequency domain, the pixels are converted into coefficients, and the secret message is inserted into these coefficients.

Spatial domain

Steganography in spatial domain (Swain, 2016) consist to change the pixels values of the image. The LSB algorithm is one of the simplest and most widespread techniques. In the LSB we hide a secret message in the lower bits of the pixels of the image, so that the distortions introduced by the insertion process are not noticeable to the human eye.

Frequency Domain

In the frequency domain (Sheisi & al, 2012) the message is inserted into the transformed coefficients of the image, which has the effect of providing more robustness against attacks. The frequency steganography is an essential technique of concealing secret information and nowadays, most steganographic systems operate in the frequency domain.

Diffie-Hellman key exchanges

Cryptology is a science that combines cryptography and cryptanalysis. Generally, encryption methods require encryption keys. An encryption key is a set of values that can encode and decode data. The exchange of a secret key is fundamental in cryptography. While encrypting a large amount of data can be done only with the secret key encryption, especially if this exchange takes place in real time because of the slow public key ciphers. Now the challenge is to communicate a transmitter of the encryption key A to a destination B without a third person E can intercept it. This is where the Diffie-Hellman protocol involved (Roy & al, 2008). The exchange of Diffie-Hellman key was developed by both authors (Whitfield Diffie and Martin Hellman) in 1976, he proposed to A and B to define a secret key even if E listens to their communication.

Diffie-Hellman algorithm

It is therefore, as required by many protocols, exchange between two parties A and B a secret key K of size t (Kumar & Ravindranath, 2015). For that A and B have a finite cyclic group G and a generator of this group. Take for example the multiplicative group G (Z / pZ) * where p is a prime number and a generating element of this group. Here is how the exchange is schematically «Figure.6». The calculations are shown in the group G, so in our example modulo p.

- A chooses an integer a such that 1 <a <p - 1 and keeps it secret
- A sends (g^a mod p) to B (calculated in the group, so here modulo p).
- B chooses an integer b such that 1 <b <p - 1 and keeps it secret.
- B sends (g^b mod p) to A.
- A calculates s = B^a mod p.
- B calculates s = A^b mod p.
- A and B now have the same key

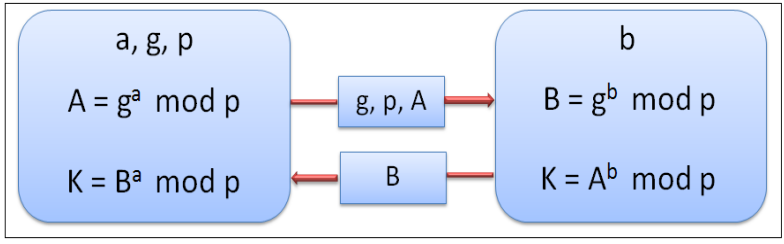

Figure 6 – The Diffie-Hellman key exchange

If a third person, for example E, listening to transmissions from A and B. In this case E has access to p, g, g^a mod p and g^b mod p. In this case, one wonders why it is not possible for E to calculate a or b to obtain the secret key. It may apparently seem simple to calculate a = $\log_g (g^a)$ or b = $\log_g (g^b)$. But this is not the case because we work here in mod p. This involves calculating a discrete logarithm. Or bitter literature, there is no quick solution to this day to calculate. E is therefore unable to determine (g^a mod p) ^{b} mod p.

P must be large enough to prevent an exhaustive search (Mandal &Parakh, 2015). Currently, using a prime number p of the order of 500-1024 numbers and a and b of the order of 100 numbers, it is impossible to determine the secret key, even with the best algorithms for solving discrete logarithm. To use this system you must build multiplicative groups (Z / pZ) *, prime numbers p and in each case a group of generating element (or at least a generator under a large group). For example SSH protocol uses numbers Sophie Germain to build these.

Weakness of the Diffie-Hellman key exchange

The biggest problem when using the Diffie-Hellman key exchange is the attack of the man in the middle (Goyat & Malik, 2013). This attack allows an attacker E to insert in the communication between A and B, he create a common key with A and do the same with B. So A and B think that they communicate directly when in reality each therefore communicates with E. In this attack E exploits a lack of identification between A with B. The protocol Station to Station (STS) for example combine the Diffie-Hellman key exchange with the public key signature, ensuring mutual authentication of the two parties so as to avoid the attack man in the middle.

Diffie-Hellman key exchange applications

Programming language

To implement our application we used the Java language, Java is a general programming language developed by Sun Microsystems its syntax is close to the C (Raval, 2013). Its characteristics and its rich ecosystem and its community have enabled it to be widely used for the development of very disparate types of applications. Java is particularly widely used for the development of business and mobile applications. We chose this language for several reasons:

- 97% of business machines have a JVM installed
- Java is downloaded over a billion times each year
- There are over 9 million Java developers worldwide
- Java is one of the most used languages in the world
- More than 3 billion mobile devices can implement Java
- More than 1.4 billion smart cards using Java are produced each year

LSB method (least significant bit)

The LSB method (Emar & al, 2016) used substitutes the two significant bits of the pixels values coding an image « Figure.7 ». A Bitmap image is an array consisting of a set of pixels. For each pixel, the color is coded with three bytes: one for red, one for green and one for blue (Khorsheed, 2014). Each byte indicates the intensity of the corresponding color, on a level from 0 to 255. Move from one level N to a level N - n, where n is very small changes slightly the color and this is precisely on which is based LSB method. If we take a byte corresponding to one of the three colors of a pixel (for example 01101011), and we change the last bit, it does not change much the color (Singh, 2015). In our example (01101011), 1 corresponds to the least significant bit. The idea is to replace the least significant bit by that information that we wish to conceal.

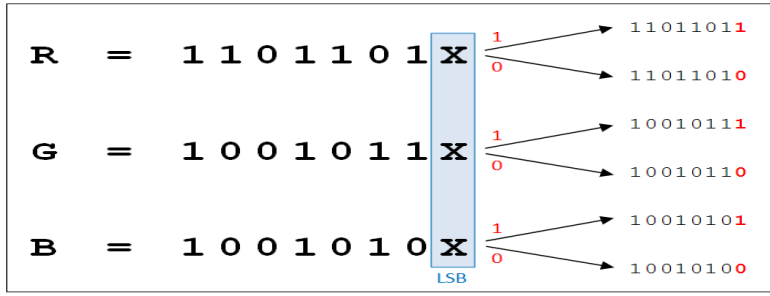

Figure 7 – Least significant bit process

Key exchange process

In our application, the user begins by connecting via a user name and an IP address « Figure.8 », the list of users connected to the network is shown to him. Then, he selects the user with whom he wishes to exchange a key and an image to be transmitted.

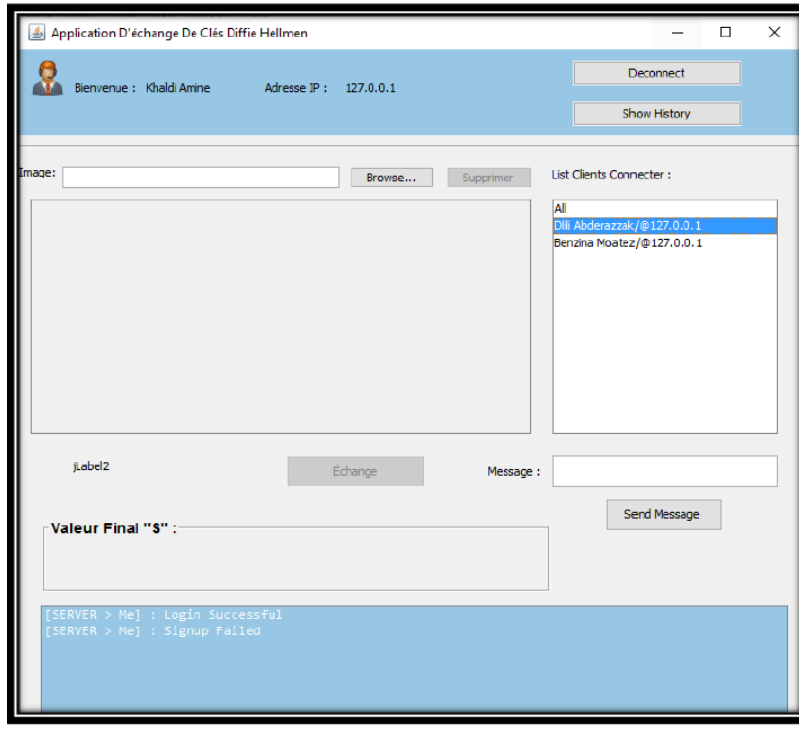

Figure 8 – Main application interface

Once these parameters chosen and approved, a tripling of prime numbers P, Q and a is generated, A is calculated ($A= P^a \% Q$). The triple A, P and Q are then hidden by the LSB steganography algorithm in the previously selected image by the LSB algorithm and transmitted to the user B « Figure.9 ».

Upon receipt of the image, B extract the triple A, P and Q, then it generates a prime number b and calculates B ($B= P^b \% Q$), the result is hidden by the LSB algorithm in the image and transmits to A.

After these exchanges, both part A and B have all the necessary information to calculate the key "S". User B will calculate $S= A^b \% Q$ and user B calculates $S= B^a \% Q$. The calculated key will be identical for both users « Figure.10».

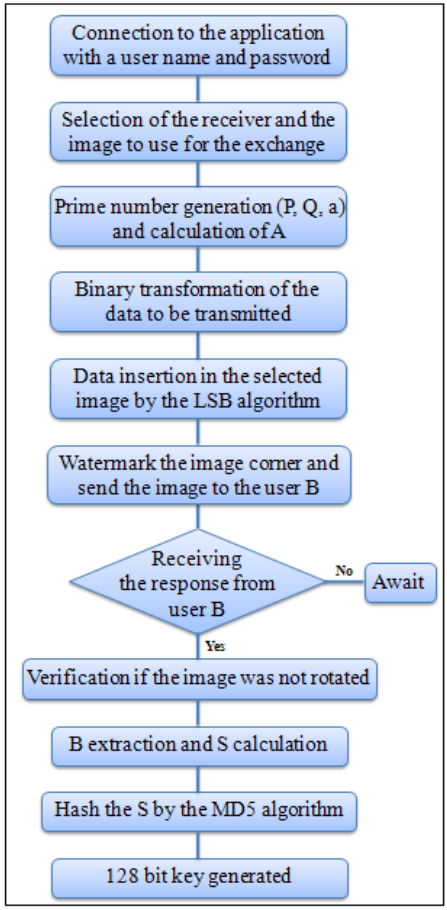

Figure 9 – Diffie-Hellman key exchange algorithm

A hash is done on the key S using the MD5 algorithm (Marakeby, 2013) which allows us to obtain a 128-bit key. The hash of the same message still generates the same result, so the same key will be generated.

Before any transmission a digital watermarking is performed on the image, it allows us to label the right corner of the image. The receiver should check this watermark before any extraction to prevent any rotation of the image, if the watermark is not on the right corner the receiver will rotate the image before data extraction. This mechanism makes our steganography invariant to rotation.

Figure 10 – Key generation

This application provides a reasonable calculation time and the changes to the image are not perceptible « Figure.11 », however, it only uses Bitmap images that are heavy images, and little used today. We worked on images that are not compressed. If our image is compressed in a destructive format like JPEG, concealed information will be lost.

(a) (b)

Figure 11 – Steganography transparency. (a) The original image. (b) The stéganographied image

Conclusion

In this paper we have presented a new approach for the Diffie-Hellman key exchange. This exchange does not require the establishment of a secure channel or a digital signature for authenticating users and avoid a man-in-the-middle attack. The use of steganography allowed us to realize the information transfer and the establishment of a symmetric key discreetly and secretly. This application modifies the last significant bit values (RGB) of a bitmap file (Spatial domain). To improve this application, we could use a JPEG file and hide the message in the DCT coefficients of this file, these images are more used and more widespread on the Internet.

References

Bresson Emmanuel, Olivier Chevassut, David Pointcheval (2007). Provably secure authenticated group Diffie-Hellman key exchange, ACM Transactions on Information and System Security, Volume 10 Issue 3, pp. 497-514.

Dagar Sunny, Vinay Kumar, Yogendra Bagoriya (2013). Image Steganography using Secret Key & Gray Codes, International Journal of Innovative Technology and Exploring Engineering, Volume 2, No 5, pp. 241-248.

Dittmann Jana, David Megías, Andreas Lang, Jordi Herrera-Joancomartí (2006). Theoretical Framework for a Practical Evaluation and Comparison of Audio Watermarking Schemes in the Triangle of Robustness, Transparency and Capacity, Lecture Notes in Computer Science, Volume 4300, pp. 1-40.

Emar Marwa, Abdelmgeid Aly, Fatma Omara (2016). An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection, International Journal of Advanced Computer Science and Applications, Volume 7, Issue 3.

Goyat Neeraj, Annu Malik (2013). Review of Diffie–Hellman key Exchange, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, pp. 285-289.

Khorsheed Omeed Kamal (2014). A review search bitmap image for sub image and the padding problem, International Journal of Advances in Engineering & Technology, Volume 7, Issue 3, pp. 684-691.

Kumar Randhir, C.C Ravindranath (2015). Analysis of Diffie Hellman Key Exchange Algorithm with Proposed Key Exchange Algorithm,

International Journal of Emerging Trends & Technology in Computer Science, Volume 4, Issue 1, pp. 40-43.

Mandal Sayonnha, Abhishek Parakh (2015). Implementing Diffie-Hellman key exchange using quantum EPR pairs, SPIE Proceedings: Quantum Information and Computation, Volume 9500, Maryland, United States.

Marakeby A. L. (2013). Analysis of MD5 Algorithm Safety against Hardware Implementation of Brute Force Attack, International Journal of Advanced Research in Computer and Communication Engineering, Volume 2, Issue 9, pp. 3332-3335.

Mstafa Ramadhan, Christian Bach (2013). Information Hiding in Images Using Steganography Techniques, Northeast Conference of the American Society for Engineering Education, Norwich University, United States.

Raval Abhilasha (2013). A Study on Buzzword in Java, International Journal of Advance Research in Computer Science and Management Studies, Volume 1, Issue 2, pp. 1-5.

Roy Arnab, Anupam Datta, John C. Mitchell (2008). Formal Proofs of Cryptographic Security of Diffie-Hellman-Based Protocols, Lecture Notes in Computer Science, Volume 4912, pp. 312-332.

Sharma Ruchika (2015). Implementation of Steganogrphy using Recursive Equation Approach, International Journal of Computer & Mathematical Sciences, Volume 4, No 2, Special Issue, pp. 15-19.

Sheisi Hossein, Jafar Mesgarian, Mostafa Rahmani (2012). Steganography: Dct Coefficient Replacement Method and Compare With JSteg Algorithm, International Journal of Computer and Electrical Engineering, Volume 4, No. 4, pp. 458-462.

Singh Amritpal (2015). An improved LSB based image steganography technique for RGB images, Electrical Computer and Communication Technologies (ICECCT2015) IEEE International Conference, Coimbatore, India.

Singh Rashi, Gaurav Chawla (2014). A Review on Image Steganography, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, pp. 686-689.

Siper Alan, Roger Farley, Craig Lombardo, (2005). The Rise of Steganography, Proceedings of Student/Faculty Research Day, CSIS, Pace University, New York, United States.

Sumathi C.P, T.Santanam, G.Umamaheswari (2013). Study of Various Steganographic Techniques Used for Information Hiding, International Journal of Computer Science & Engineering Survey, Volume 4, No. 6, pp. 9-25.

Swain Gandharba (2016). Digital Image Steganography Using Variable Length Group Of Bits Substitution, International Conference on Computational Modelling and Security (CMS 2016), Volume 85, pp. 31-38.

Takebe Hirotoshi, Keisuke Tanaka (2013). Grey-Box Public-Key Steganography, Lecture Notes in Computer, Volume 7876, pp. 294-305.