Design and Implementation Multi Level Security System

Saba Mohammed Husain
Information technology college-Babylon university
Saba_muh@ymail.com

Abstract

Today the security becomes an important issue of communication and the need of it information has become a necessity. The proposed article provides a method encrypts text and hide it inside a digital image. This article included many stages where the first stage reverse the plain text while in the second stage the text is encrypted using a Groth algorithm and third stage is hide the text inside digital image using the method of least significant bit where cipher text is spread inside bits of color bands (RGB)in a manner that does not affect on the final image, this method is considered more effective and ease in hiding process.
Keywords: security, cryptography, Groth.

الخلاصة

اصبحت امنية المعلومات في عصرنا الحالي موضوعا هاما وضرورة ملحة في علم الاتصالات. يوفر البحث المقترح طريقة لتشفير النص واخفائه داخل صورة رقمية. تتضمن عملية التشفير هذه عدة مراحل: في المرحلة الاولى يتم اجراء عملية عكس للنص العادي، اما المرحلة الثانية فتتضمن تشفير النص اعتمادا على خوارزمية groth بينما تتكفل المرحلة الثالثة باخفاء النص داخل الصورة الرقمية باستخدام البت الاقل اهمية بحيث ان البتات المشفرة توزع داخل بتات الحزم اللونية RGB بطريقة لا تؤثر على الصورة النهائية. تعتبر هذه الالية اكثر فعالية وسهولة في عملية الاخفاء.
الكلمات المفتاحية: الامنية، تشفير، طريقة تشفير Groth.

Introduction

Steganography is not the same as cryptography. The primary goal of cryptography is to secure interchanges by exchanging the information into a structure so that it can't be seen by a meddler. Then again, steganography strategies have a tendency to shroud the presence of the message itself, which makes it troublesome for an eyewitness to make sense of where precisely the message is, (Shikha Sharda2013).

System security is imperative at the present time as the quantity of information traded developments with on the web. Consequently, the security and dependability of the information that needs to ensure close to unapproved get to and utilization. This is making it increasingly in the field of hiding information. In addition, the broadcast technology and the rapid deployment also requires an alternative solution to hide the information. To guarantee copyright, for example, sound, feature and other source accessible in advanced structure may prompt unapproved replicating on an expansive scale. The copyright, for example, sound, feature and other source accessible in computerized structure may prompt huge scale unapproved duplicating. This is on account of the computerized configurations make conceivable to give high picture quality even under multi-replicating. In this manner, the exceptional piece of imperceptible data is altered in every picture that couldn't be effortlessly extricated without specific procedure sparing picture quality at the same time, (Provos, 2001).

While cryptography is skirting on keeping the substance of messages (their criticalness), steganography is basically hiding the message so that middle person persons can't see the message. Steganography insinuates data or a record that has been concealed inside an electronic Picture, Video or Audio archive. Pictures can be

more than what we see with our Human Visual System (HVS); therefore, they can go on more than only 1000 words, (Vijaykumar Sharma2012).

Overview Steganography

The word Steganography is of Greek source and signifies "disguised composition" from the Greek words steganos signifying "secured or ensured", and graphein signifying "to compose". The initially recorded utilization of the period was in 1499 by ""Joharnnes Trithemius"" in his Steganographia, a treatise on cryptography and steganography camouflaged as a book on enchantment, (Sravanthi, 2012).

The inspiration driving creating picture Steganography systems as indicated by its utilization in different associations to impart between its individuals, and in addition, it can be utilized for correspondence between individuals from the military or insight agents or operators of organizations to shroud mystery messages or in the field of undercover work. The primary objective of utilizing the Steganography is to abstain from attracting gattention to the transmission of shrouded data. In the event that distrust is raised, then this objective that has been wanted to accomplish the security of the mystery messages, in light of the fact that if the programmers noticed any adjustment in the sent message then this onlooker will attempt to know the concealed data inside the message,(Wang, 2010; Corporation, 2005).

The essential model of steganography comprises of Carrier, Message and Password. Transporter is otherwise called spread article, which the message is inserted and serves to shroud the vicinity of the message. Essentially, the model for steganography is the message is the information that the transmitter wishes to remain it private. It can be plain content, figure content, other picture, or anything that can be implanted in a bit stream, for example, a copyright check, a clandestine correspondence, or a serial number. Watchword is known as stego-key, which guarantees that just beneficiary who know the comparing unraveling key will have the capacity to concentrate the message from a spread article. The spread article with the covertly inserted message is then named the stego-object steganography systems that install concealed messages in sight and sound items have been proposed, (Johnson, 2003).

Stenographic Techniques

There are a considerable amount of methodologies in arranging stenographic methods. These methodologies can be characterized as per the sort of spreads utilized with mystery correspondences. Another plausibility is done by means of sorting such methodologies relying upon the sort of spread change officially connected during the time spent implanting. The second approach is embraced in this work ,albeit at times a careful order is impractical, (Kruus, 2003).

Stream generators

direct criticism movement registers are broadly utilized as a part of key stream generators in light of the fact that they are appropriate for equipment execution, produce successions having expansive periods and great measurable properties, and are promptly investigated utilizing logarithmic systems.

For basically all conceivable mystery keys, the yield grouping of a LFSR-based key stream generator ought to have the accompanying properties:

1. extensive period.

2. extensive straight multifaceted nature.
3. great measurable properties .

It is underlined that these properties are just fundamental conditions for a key stream generator to be considered cryptographically secure. Since numerical confirmations of security of such generators are not known, such generators must be considered computationally secure.

Proposed Technique Steps

- Reverse the plain text

In the first of proposed technique is reverse the plain text where the first symbol will be the last symbol, this step adds more active to the security for secret message.

- Convert the plain text to binary.

The plain text will be generated to the ASCII code then transformed it to the series of zeros and ones

- Encrypted the series of binary

Growth algorithm

This algorithm consists of the shift of one registered with a feedback function linear, characterized by the output of these registers as the result of group operations is in progress on the content of the group stages are as follows

Stage 8 and stage 5 share operation (and)
Stage 7 and stage 3 share operation (and)
Stage 6 and stage 1 share operation (and)
Stage 4 and stage 2 share operation (and)
The output of the previous processes share process (XOR) The following diagram shows this linkage.

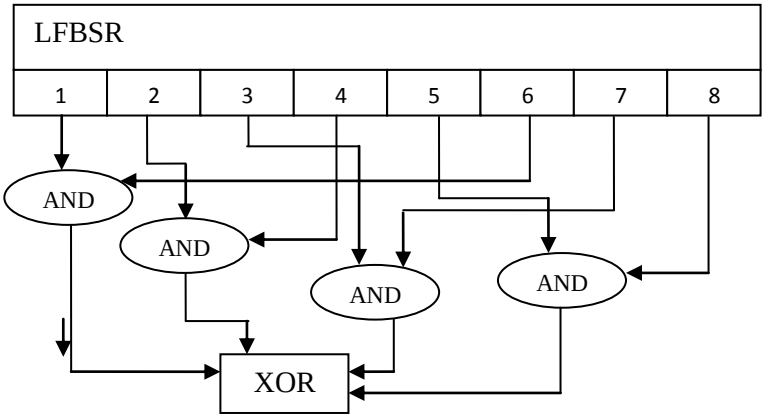


Figure (1) Groth system

At the end of Groth system key is generate sequence of zeros and ones. The resulted key XOR with the reverse plain text (binary) to obtain the encrypted text.

Hiding the encrypted text

In this step the LSB is used to hide the encrypted text in cover image as following

Encrypted text 110010101100……

Cover pixels	11001010	11001011	10101010	11001100	10110011	11100011
	R	G	B	R	G	R
stego pixels	11001011	11001000	10101010	11001110	10110011	11100000
	R	G	B	R	G	R

- Send the stego-image

PSNR (Peak Signal-to-Noise Ratio)

The way of the stego pictures has been measured using PSNR (Peak Signal-to-Noise Ratio). PSNR is a standard estimation used as a part of steganography technique to test the way of the stego pictures. The higher the estimation of PSNR, the more quality the stego picture will have. In case the spread picture is C of size M × M and the stego picture is S of size N × N, then every spread picture C and stego picture S will have pixel regard (x, y) from 0 to M-1 and 0 to N-1 independentlThe PSNR is then c:

$$PSNR = 10.\log_{10}\left(\frac{MAX^2}{MSE}\right) \qquad (1)$$

wher

$$MSE = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(C(x,y)-S(x,y))^2$$

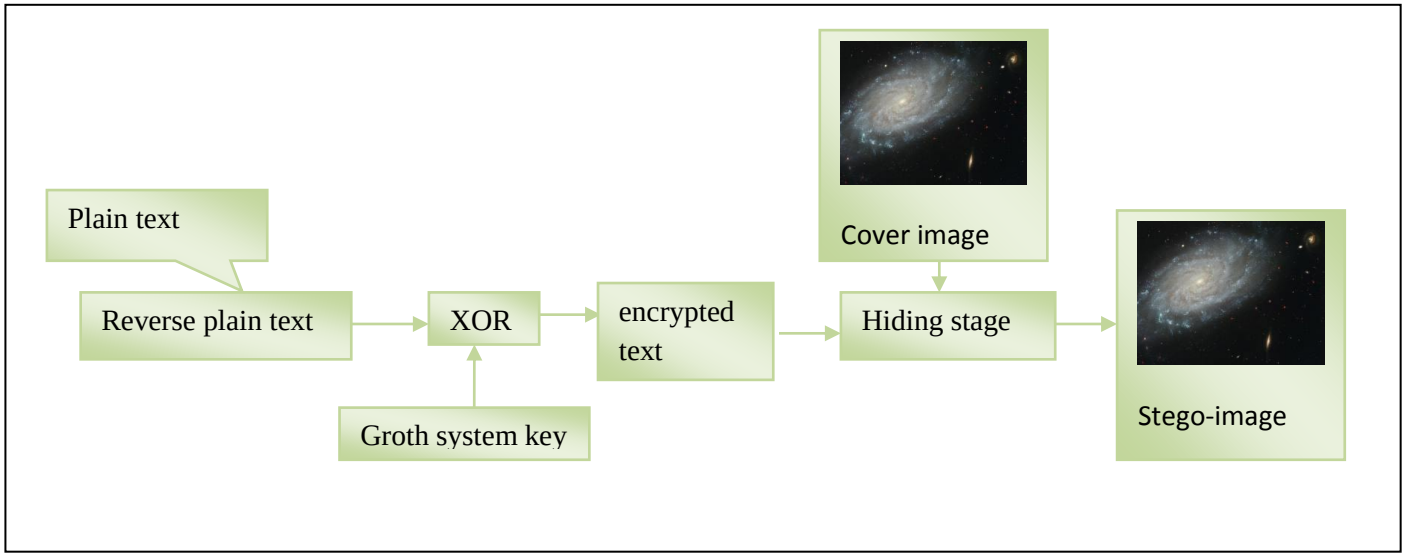


Figure (2) suggested system

Simulation And Resu

In this article, the plain text is reverse and encrypted by Xoring with Groth system key and hiding in the cover image, the PNSR and the histogram are computing to ensure that the stego-image will never different from the original image and the result as the following:

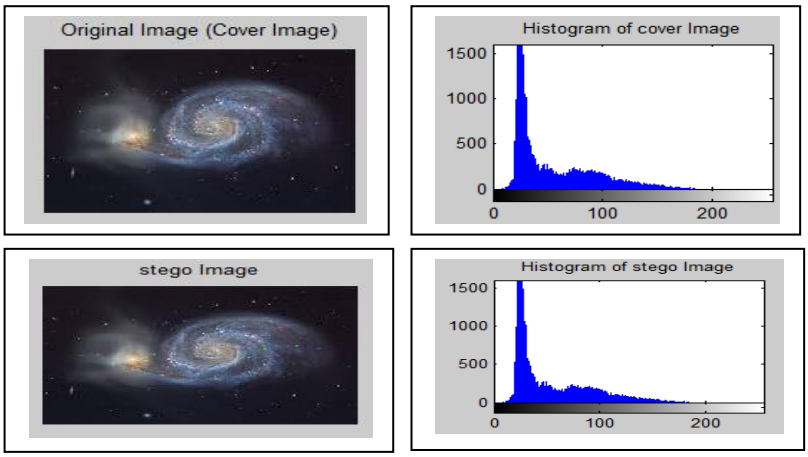


Figure (3) shows the first experiment histogram and PSNR is 82.8969

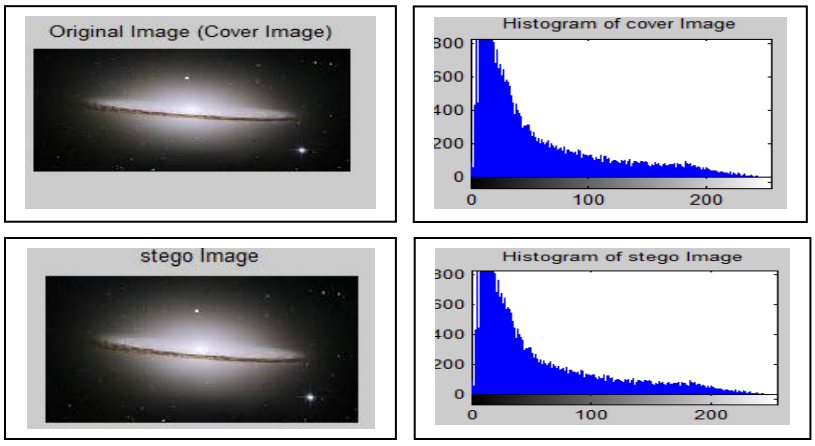


Figure (4) shows the first experiment histogram and PSNR is 88.1994

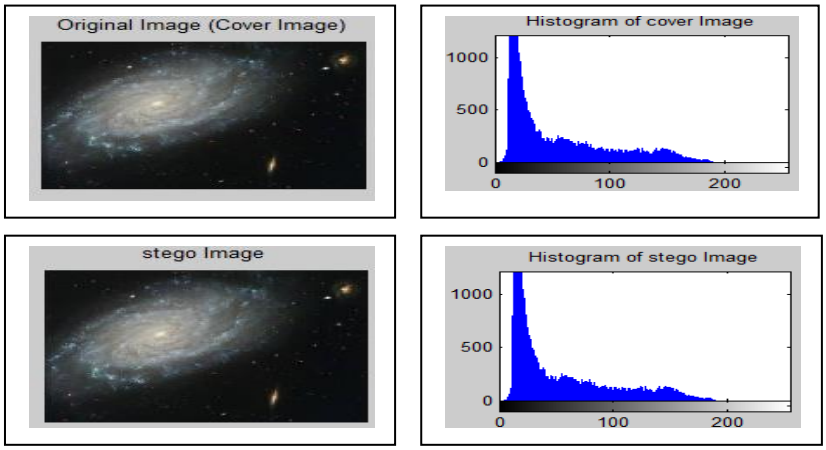
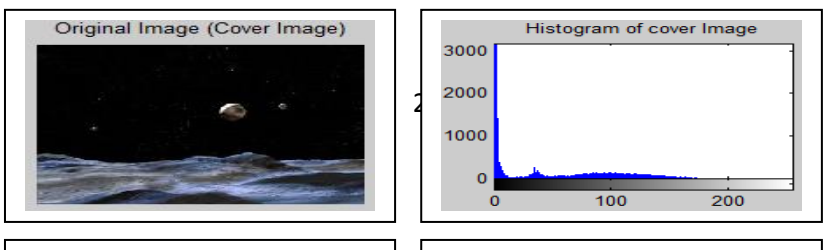


Figure (5) shows the first experiment histogram and PSNR is 80.1353



Conclusion

The histogram show that there is invisible difference between the stego image and clear image or original image. The reversing for the plain text increase the security of the system. For more secure the resulted text encrypted using growth algorithm. The using of LSB with groth algorithm increases the level of security.

References

Available: http://www.isso.sparta.com/documents/asrjv5.pdf#page=47 [Oct., 2011].

Johnson N.F. & S. Jajodia, 2003,"Steganalysis of Images Created Using Current Steganography Software", in *Proceeding for the Second Information Hiding Workshop*, Portland Oregon, USA, April 1998, pp. 273-289.

Kruus, P.; C. Scace, M. Heyman, and M. Mundy. (2003), "A survey of steganography techniques for image files." Advanced Security Research Journal. [On line], 5(1), pp. 41-52.

Provos, N. January 31, 2001,"Probabilistic Methods for Improving Information Hiding", *CITI Technical Report 01-1*.

Shikha Sharda1, Sumit Budhiraja2, 2013, "Image Steganography", International Journal of Emerging Technology and Advanced Engineering Website, (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013) 707 .

Sravanthi, G.S.; Mrs.B.Sunitha Devi, S.M.Riyazoddin &M.Janga Reddy , 2012, "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", Global Journal of Computer Science and Technology Graphics & Vision ,Volume 12 Issue 15 Version 1.0. (USA).

Vijaykumar Sharma , Vishal Shrivastava, 15th February 2012, A STEGANOGRAPHY ALGORITHM FOR HIDING IMAGE IN IMAGE BY IMPROVED LSB SUBSTITUTION BY MINIMIZE DETECTION, Journal of Theoretical and Applied Information Technology, Vol. 36 No.1 © 2005 - 2012 JATIT & LLS. All rights reserved.

Wu, H.; H. Wang, C. Tsai and C. Wang, 2010)," Reversible image steganographic" . scheme via predictive coding. 1 (, ISSN: 01419382, 35-43. J, Corporation, 2005, "Steganography". http://www.webopedia.com/ TERM/S/steganography.html.