نظام مقترح لإخفاء البيانات باستخدام تقنية
# Steganography

ا.م بيداء جعفر الخفاجي,,مهيب طارق حسين ,م. د مي عبد المنعم صالح م. م شيماء عبد الحسين ,

جامعة بغداد\كلية التربية ابن الهيثم\قسم الحاسبات

جامعة بغداد\كلية التربية ابن الهيثم\قسم الحاسبات

جامعة بابل\كلية التربية الاساسية\قسم الرياضيات والحاسبات

جامعة بابل\كلية التربية الاساسية\قسم الرياضيات والحاسبات

## Proposed System for Data Hiding Using Steganography

**Baydaa Jaffer AlKhafaji ,    Moheeb Tariq Hussein ,May A. Salih,   ,Shaymaa AbdulHussein**

**Computer Science Department, College of Education for Pure Science/Ibn Al-Haitham, University of Baghdad,**

**Computer Science Department, College of Education for Pure Science/Ibn Al-Haitham, University of Baghdad,**

**Math and Computer Science Department, Basic Education College, University of Babylon, Hilla,**

**Math and Computer Science Department, Basic Education College, University of Babylon, Hilla,**

Baydaa .j.s@ ihcoedu.uobaghdad.edu.iq, bjkh68@yahoo.com ,

Baydaa.khafaji@gmail.com

Username.mt77@gmail.com

may.abd@uobabylon.edu.

Shaymaahusain2015@gmail.com

## Abstract

Steganography is the science that serves to hide a specific message in a suitable cover file without making a noticeable changing with the cover that brings an attention or HSS (Human Sense System) in both (Human Visual System-HVS and Human Auditory System-HAS) and/ or computer detecting software which leads to stegano analysis.

Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data Computer-based steganographic techniques introduce changes to digital cover to embed information foreign to the native covers Such information may be communicated in the form of text, binary files, or provide additional information about the cover and its owner such as digital watermarks or finger prints.

**Keyword**  steganography **,** LSB**,** watermarking, Cryptography.

الملخص

النظام المقترح  هو اخفاء نص في صورة، ويتكون هذا النظام المقترح من أربع مراحل صورة ستكون تلك الإطار المقترح ، وهذا الإطار يتكون من المطالبة بأربع مراحل ، مرحلة المعالجة التمهيدية ، مرحلة التضمين ، مرحلة الاستخراج ، مرحلة ما بعد المعالجة. كل مرحلة قد تكون مكملة لمرحلة المعالجة المسبقة تتألف من

مرحلتين، تلك التي تبدأ سيتم تحويل المرحلة، والتي تتغير أكثر. تلك الثانية ستكون مرحلة الترميز، التي رمز تلك المعلومات المدرجة. تلك المرحلة التضمين يأخذ المعلومات المدرجة، والتي في هذا الإطار الموصى به عملية الاخفاء. (ملف نصي) وكائن الغلاف الذي سيكون ربما صورة مخطط بت (bmp) أو توافق الرسومات. تنسيق (gif) الصورة ثم الفجوة تلك الثنائية الغطاء تحت N –كتل كل مربع تحتاج إلى مدى [8 * 8] خلاف ما هو أكثر من ذلك. وجاء إخفاء كل لمسة حول البدء مع مرحلة الترميز في تلك ( 1,2,3 ما هو أكثر 4)

## Introduction

Every few years computer security has to re-invent itself. New technologies and applications bring new threats, and force us to invent new protection mechanisms. Cryptography became important when business started to build networked computer systems; virus epidemics started once large numbers of pc users were swapping programs, and when the internet took off , the firewall industry was one of the first to benefit[1].   One of the hot spots in security research is information hiding. It is driven by two of the biggest policy issues of information age copyright protection (watermarking) and state surveillance (steganography). Steganography's intent is to hide the existence of  a hidden message, the goal of steganography is to hide message inside other harmless message in a way that does not allow any enemy to even detect that there is a second secret message present.  While watermarking and fingerprinting are used to protect authors, artist, software and things have copyrights.  Placing a hidden trademark in products is watermarking, and hiding a serial number or a set of characteristics that distinguishes an object from a similar object is fingerprinting.  They are both used to fight piracy, to detect and prosecute any violators [2].

## History of  Steganography

Steganography is very old method of passing a message in secret.  This method of message sending goes back to the  ancient Greeks.  The historian Herodotus wrote about how an agent wrote a message of an invasion on the wood part of a wax tablet.  Since message was normally inscribed in the wax and not the wood, the tablet appeared blank to a common observer[3].  Another famous example of a classical system is that of the roman general who shaved the head of a slave and tattooed a hidden message on it . After the hair had grown back, the slave was sent to deliver the message. While such a system might work once, the moment that it is known, it is simple to shave the heads of all people passing by to check for hidden message[4].    Another common form of invisible writing is through the use of invisible inks. Such inks were used with much success in both World War I and World War II [5].

## Use Of  Steganography

There are many reasons why steganography is used, and it is often used in significant fields. It can be used to communicate with complete freedom even under conditions that are censured or monitored . it can also be used to protect private communications where the use of the cryptography is normally not allowed or would raise suspicion. In the following some reason why use steganography

-Allows people to communicate secretly by establishing a secret communication protocol.

-Allows non-authorized communication through authorized communicatirewall [6].

## Least Significant Bit

The least significant bit insertion method is probably the most well known image Steganography technique. It is a common, simple approach to embedding information in a graphical image file.

The embedding process consists of choosing a subset $\{j_1, \ldots, j_{l(m)}\}$ of cover elements and performing the substitution operation $c_{ji} \leftrightarrow m_I$ on them, which exchanges the LSB of $c_{j1}$ by $m_i$ ($m_i$ can either be 1 or 0). One could also imagine a substitution operation which changes more than one bits of one-cover element. In the extraction process, the LSB of the selected cover-elements are extracted and lined up to reconstruct the secret message.

The following program performs data hiding in one least significant bit (1 LSB) after encoding it:

```
for(int ze=0;ze<8;ze++)
 r[m][ze]=temp[ze];
            }va=7; m=0;
       for(;;)
      {if (m= =8) break;
        switch (m)
              {case 0:
         case 1:
             case 2:
             case 3:
             case 4:
             case 5:
             case 6:
         case 7:va=7; break;}
                while (va= =7)
               {if (code.good())
                   max=code.get();
               switch (max)
                  {case 48:f=0;
                   cod=f+1;
            r[m][va]=cod; break;
               case 49:f=1;
          cod=(f+1)%1;
             r[m][va]=cod; break;}
                ++va; if (va==8) ++m;}
```

## conclusion

Steganographic images have large capacities in which to hide data.    We've chosen to use BMP for the proposed system because they are of a very simple format and very easy to work with compared to other formats such as GIF and JPEG. Using cryptography add a level of security/secrecy to the proposed system, so if a hidden message is encrypted, it must also be decrypted if discovered.

## References

[1] Kharrazi, M., Sencar, H. T., and Memon, N. (2004). Image Steganography: Concepts and practice. In WSPC Lecture Notes Series

[2] Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and Applications

[3] D.R. Stinson, Cryptography: Theory and Practice, Boca Raton, CRC Press, 1995.

[4] Provos, N. and Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE SECURITY &PRIVACY

[5] Chandramouli, R., Kharrazi, M. & Memon, N., "Image Steganography and teganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

[6] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002

[7] Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999

[8] BJ AlKhafaji, MA Salih, S Shnain, Z Nabat,segmenting video frame images using genetic algorithms,2020 Periodicals of Engineering and Natural Sciences 8 (2), 1106-1114

[9] BJ AlKhafaji, M Salih, S Shnain, Z Nabat ,improved technique for hiding data in a colored and a monochrm images,2020, Periodicals of Engineering and Natural Sciences 8 (2), 1000-1010

[10] AL-Khafaji, B.J. Image Improvement Using The Combination of Wavelet and Multiwavelet Transform. *Ibn Al-Haitham Journal For Pure And Applied Science.***2010**, *23*, *3*, 275-282.

[11] Al-Khafaji, B.J. DetectTheInfected Medical ImageUsing Logic Gates. *Ibn Al-Haitham Journal For Pure And Applied Science.***2014**, *27*, *2*, 260-267.