# DuoHide: a Secure System for Hiding Multimedia Files in Dual RGB Cover Images

Marwa Tariq Al-Bayati
Dept. of Computer Science
Middle East University
Amman, Jordan
e-mail: marwa.albayati@outlook.com

Mudhafar M. Al-Jarrah
Dept. of Computer Information Systems
Middle East University
Amman, Jordan
e-mail: maljarrah@yahoo.com

***Abstract*—Steganography, the technology of protecting a secret message by embedding it inside a cover image, continues to be investigated and enhanced as an alternative data protection method. This paper deals with hiding multimedia files in true color RGB cover images with an emphasis on reducing the cover size, increasing hiding capacity and enhancing security of the hidden data. A proposed model (DuoHide) is presented in which a secret multimedia file, regardless of its type, is processed without un-compression, and divided between two cover images of equal size and dimensions. The multimedia file is read as a stream of bytes and split vertically into two parts; one part contains the least significant half-bytes, and the other part contains the most significant half-bytes. The two parts are hidden inside two uncompressed RGB cover images using a least significant 4-bit replacement technique. The resulting dual stego images are expected to be sent separately, through different channels, to avoid capture of both stego files by an adversary. Extraction of the secret file is achieved through merging LSB half-bytes from the two stego files. The extracted file is identical in content and structure with the original secret file. The implemented DuoHide system was evaluated using a set of public multimedia files; images, audios, and videos, of various sizes. The secret file sizes ranged from 5% to about 100% of the cover image's size. The experimental results showed that even at the highest embedding ratio, which is based on the secret-to-cover ratio, there were no perceptible visual differences between cover and stego images. The PNSR value was calculated as PSNR1, for cover1 and stego1, and PSNR2 for cover2 and stego2. The lowest PSNR value was around 31 dB for the highest embedding ratio, which is considered acceptable concerning statistical imperceptibility. The PSNR value increased as the embedding ratio decreased, reaching around 65 Decibel (dB) for the case of 5% secret-to-cover ratio. The integrity of the extracted secret file was verified through a bitwise comparison between original and extracted files, which showed zero differences.**

**The DuoHide model is expected to provide better security for the hidden file, in case an attacker manages to capture one of the stego images and recover the hidden content because the attacker will only get an incomprehensible set of half-byte bits. An additional advantage of using a pair of stego files is that of reducing stego file size by 50%, to avoid problems and limitations of transmitting large files, especially that multimedia files are often large, and they cannot be compressed because they are already compressed. Security of the DuoHide system can further be improved by randomizing storage locations within the two stego images.**

***Keywords—steganography; dual hiding; secret-to-cover ratio; vertical splitting; PSNR; cover image; stego image; multimedia file.***

## I. INTRODUCTION

The nature of data exchanged over the internet, whether for social networking or business communication, has changed recently from short text messages to various types of multimedia files such as video clips, audio recordings, photographic albums, maps, and engineering and scientific images. Many of such documents contain confidential information that is targeted for capture by adversaries, industrial espionage hackers, business competitors, paparazzi and personal data hackers.

Securing multimedia data requires preventing unauthorized users from access, distortion, destruction, detection or modification of the data during its transfer. There are two primary methods for data security protection, encryption, and steganography. The encryption method protects data by converting it to an unclear form that cannot be perceived by attackers. Cryptography techniques have two drawbacks: (i) knowledge about the use of cryptography in a targeted system could lead to attempts by adversaries to break the encryption and decipher the encoded data, and (ii) the key management overhead imposed on the user. The second method of data security is steganography, which conceals the presence of the secret data by hiding it inside cover documents (files) of various types such as text, image, audio, and video. Three objects are involved in the concealment (embedding) process; the secret file, the original cover file and the stego file which combines the secret and the cover files [1]. The hiding of secret data is carried out by mixing bits of the secret information with bits of the cover document in such a way that an observer or an attacker will not notice a perceivable change in the cover document. A data hiding system consists of two processes; the embedding process, which embeds the secret file inside the stego file, and the extracting process which recovers the embedded secret file. Some data hiding schemes use lossy compression, to allow for higher hiding capacity at the expense of loosing bits of the secret file.

The work in this paper presents a data hiding technique for the protection of multimedia files, through embedding in dual cover (stego) RGB images, with the aim of reducing the cover

978-1-5090-5487-9/17 $31.00 © 2017 IEEE
DOI 10.1109/DeSE.2016.23

image size, increasing the hiding capacity, and protecting the secret file through a safe partitioning scheme.

## II. HIGH CAPACITY HIDING

Multimedia files are usually larger than text and still image documents, hence require higher embedding space within cover files. One approach for reducing the hiding capacity requirements is to compress the data, as in the work in [2]. However, most multimedia files, are already compressed; as with audio and video files, therefore, further compression can result in obvious sound or video distortion.

The least significant bit (LSB) technique is a suitable choice for high capacity hiding that does not involve compression, as it provides large redundancy area for embedding in the cover medium [3]. There have been several alternatives of the LSB method regarding the number of least significant bits per pixel or element of a pixel that can be replaced, such as 1-bit, 2-bit, 3-bit, and 4-bit LSB. Also, the cover image can consist of one byte per pixel, as in grey-scale images, or of three bytes as in RGB images. In RGB images, some stego techniques change only the LSB of the right most byte (the blue channel), while others change the LSB of every color channel [4]. The use of 4-bit LSB for embedding in the three color channels gives 50% hiding capacity within the available data area, which has been shown to give acceptable visual imperceptibility between cover and stego images [5].

To increase the embedding space that is needed for hiding a large multimedia file, either a larger cover is used, or multiple covers are used. Increasing cover size has its drawbacks, due to file size limitations on email and file transfer systems. Therefore, it is more practical to split the secret multimedia file over several covers, which will reduce the required covers' sizes, but what is the good number of covers. Increasing the number of covers results in more overhead for managing multiple covers, while reducing the number of covers will require larger covers. In the present work, dual covers are chosen for hiding a secret multimedia file, which can be upgraded to four covers if necessary.

## III. SECURITY OF EMBEDDED DATA

Although data hidden within stego files are considered to be safe from access by adversaries, however, additional measures of protection of the hidden data is seen as necessary, due to the increase in the sophistication of steganalysis methods that can detect and even extract the hidden data [6, 7, 8, 9].

Several steganography studies have proposed to combine cryptography with steganography [10]. Adding encryption, as the second layer of protection has its drawbacks, as discussed earlier. Multi-layered (nested) embedding can enhance security, but with every additional layer, the hiding capacity is reduced. In this research we have chosen an approach of adding extra security to protect the hidden data by splitting the secret file into two fragments where each fragment on its own will not reveal any part of the hidden secret.

## IV. THE MULTIMEDIA HIDING SYSTEM

The proposed DuoHide system provides the essential functions for hiding a multimedia file in two stego RGB images, extracting the hidden file without change, and producing the necessary imperceptibility evaluation details.

The system consists of two modules, Embed, and Extract, and it is implemented in MATLAB.

### *A. Design Factors*

The following design factors have been taken into consideration:

1. Dual BMP RGB cover images are used to store the hidden multimedia files, such that each cover (stego) image will carry 50% of the hidden data. It should be possible to use the same cover image twice (as stego1 and stego2), or to use different images of equal size and dimensions.
2. The multimedia file will be processed as a stream of bytes, regardless of its format, and it should not be uncompressed if it is a compressed file.
3. The multimedia file will be split vertically into two parts, i.e. each byte is divided into two half-bytes and, each half-byte is hidden in a different cover (stego) image, the LSB half-byte can be stored in stego1 and the MSB half-byte in stego2 or vice versa.
4. The secret data half-bytes are embedded in the red, green and, blue channels of the stego images using a 4-bit least significant bit (LSB) technique, whereby the secret half-bytes replace the LSB half-bytes of the cover's color channel.
5. Extraction of the hidden file from the two stego images will result in a file that is identical in structure and content with the original secret file. A bitwise comparison between the original multimedia file and the extracted file, using Windows file compare (FC) command should result in zero differences.
6. The Peak Signal-to-Noise Ratio (PSNR) results of comparing the cover image(s) with the two stego images should be identical to results produced by an acceptable standard image comparison software such as ImageMajick (available: www.imagemajick.org).
7. The size of the RGB BMP cover image should be near equal to the size of the secret file, exceeding the secret file size by 54 bytes only, which is the BMP file header size. The Hiding Capacity (HC) of a cover image which is equal in size to the secret file will be sufficient to store half of the secret file, using the 4-LSB technique. The hiding capacity of each cover in bytes is calculated as:

$$HC = Width \times Height \times 3 / 2. \quad (1)$$

### *B. Data layout of cover images and secret multimedia files*

1. The secret multimedia file is processed as a stream of bytes; each byte consists of MSB half-byte (Left Half-Byte or LH), and the LSB half-byte (Right Half-Byte or RH) as shown in Fig. 1.

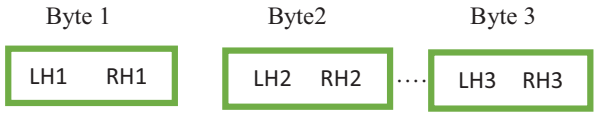


Fig. 1. Secret multimedia file as a stream of bytes

2. The dual cover images are in RGB BMP format where each pixel is stored in 24 bits, 8-bits per color channel. The right half of each color channel (the LSB half-byte) is replaced with a half-byte from the secret file, while the MSB half-byte remains unchanged, as shown in Figure 2.


Fig. 2. Stego images after half-byte replacement

## V. RESULTS and DISCUSSION

The DuoHide system was used in embedding multimedia files of various sizes, and of different formats including JPG, PNG, BMP, TIF and GIF images, as well as audio MP3 and video MP4 and WMV files. The cover images were uncompressed RGB images in BMP format, of sufficient hiding capacity for embedding the multimedia files. The dataset of cover images and multimedia files has been made available online in [11].

Each secret multimedia file is split vertically, and the two partitions are stored separately in two copies of a cover image, as stego1 and stego2. For each embedding case, the PSNR values between the cover image and the two stego image are calculated, as PSNR1 and PSNR2. Also, the secret- to-cover ratio (SCR) is calculated, which represents the ratio of the secret multimedia file size to a single cover size. The SCR metric was proposed in [10], as a useful indicator of embedding capacity utilization, to be used in conjunction with the PSNR metric.

In the following sections, statistical and visual imperceptibility results are discussed.

### *A. PSNR statisical imperceptibility results*

A large BMP cover image, Labelle.bmp[1], size 9.11 MB, and dimensions 1500x2123, was chosen as the common cover for embedding various secret multimedia files. Table I shows the PSNR and SCR metrics values of embedding a group of secret multimedia files of various sizes, inside Labelle.bmp image. The two PSNR values for each case (PSNR1 and PSNR2) are very close. The minor differences between PSNR1 and PSNR2 are due to the difference between the two halves of each byte; which leads to different accumulative effects on the stego images. The results show that even when the secret-to-cover ratio is about 100%, the PNSR value is above 31 dB, which is considered acceptable regarding imperceptibility. The highest PSNR value is 65.1278 dB, for a very small secret file with a secret-to-cover ratio of 0.05%, which suggests that PSNR value alone, without consideration to embedding ratio, is not a sufficient factor in evaluating the effectiveness of a steganography scheme.

TABLE I
PSNR RESULTS FOR LABELLE COVER (9.11 MB) WITH VARIOUS MULTIMEDIA SECRET FILES

| Secret File | Secret File Size | Secret to Cover Ratio | PSNR1 (cover with stego1) | PSNR2 (cover with stego2) |
|---|---|---|---|---|
| Krokussen.png | 9.01 MB | 98.90% | 31.9861 | 31.9863 |
| Mount-of-olives.mp4 | 8.51 MB | 93.41% | 32.0680 | 32.0660 |
| BeethovenNo9.mp4 | 8.01 MB | 87.93% | 32.3222 | 32.3268 |
| Time-Lapse.mp4 | 7.30 MB | 80.13% | 32.8569 | 32.8561 |
| MilkyWay.wmv | 6.14 MB | 67.40% | 33.2885 | 33.6805 |
| Flower.tif | 5.5 MB | 60.37% | 34.1284 | 35.3978 |
| Xynthia_anim.gif | 3.48 MB | 38.20% | 36.3457 | 36.3321 |
| Saut.mp4 | 2.68 MB | 29.42% | 37.1968 | 37.1925 |
| Elisa.mp3 | 1.46 MB | 16.05% | 39.9877 | 40.0290 |
| Poppies.jpg | 995 KB | 10.67% | 41.7511 | 41.7513 |
| Renoir2.bmp | 958 KB | 10.27% | 41.8279 | 42.6137 |
| Vase1024.jpg | 490 KB | 5.25% | 43.9881 | 43.9877 |
| Renoir4-2048.jpg | 487 KB | 5.22% | 44.7682 | 44.7764 |
| First-day-of-spring.gif | 136 KB | 1.46% | 50.2369 | 50.1603 |
| Vase128.jpg | 12.5 KB | 0.13% | 60.4890 | 60.3719 |
| Renoir4-128.jpg | 4.8 KB | 0.05% | 65.1278 | 64.9055 |

[1] *The original painting is "la Belle Ferroniere", attributed to Leonardo Da Vinci, and the digital copy was downloaded from Wikimedia.org.*

*B. Visual Imperceptibility Results*

Figures 3 to 5 show visual comparisons between the common cover image, Labelle.bmp and the two stego images, for three cases of secret multimedia files (large, medium and small files), where the large multimedia file is about the same size the cover image. The shown images represent a 20% version of the original digital images; they have been reduced for presentation purposes in this paper, but the original full images can be viewed on the dataset website [11]. Information about the secret multimedia files and the cover images are presented in the thesis in [12].

Fig. 3 shows the cover image Labelle.bmp and the two stego images; stego1, and stego2. The secret multimedia file Krokussen.png (9.01 MB), was embedded in the two stego images. The resulting PSNR values were 31.4487 (cover with stego1) and 31.4468 (cover with stego2).

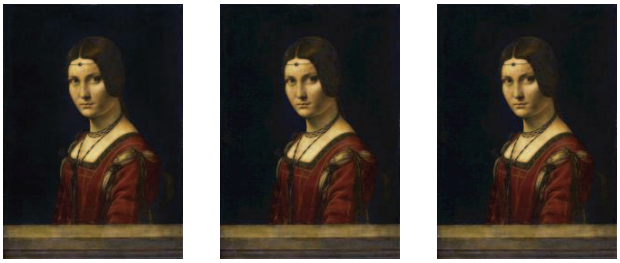


Fig. 3. Labelle.bmp embedded with Krokussen.png (9.01 MB)

Fig. 4 shows the cover image Labelle.bmp and the two stego images; stego1, and stego2. The secret multimedia file Time-Lapse.mp4 (7.30 MB), was embedded in the two stego images. The resulting PSNR values were 32.8569 (cover with stego1) and 32.8561 (cover with stego2).

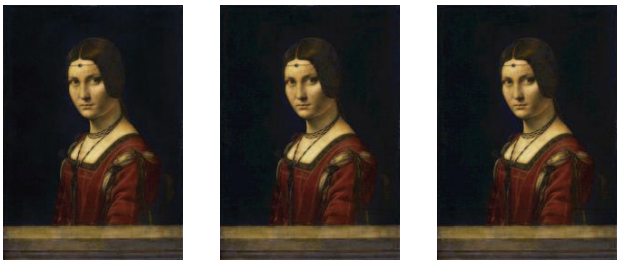


Fig. 4. Labelle.bmp embedded with Time-Lapse.mp4 (7.30 MB)

Fig. 5 shows the cover image Labelle.bmp and the two stego images; stego1, and stego2. The secret multimedia file Renoir4-128.jpg (4.8 KB), was embedded in the two stego images. The resulting PSNR values were 65.1278 (cover with stego1) and 64.9055 (cover with stego2).

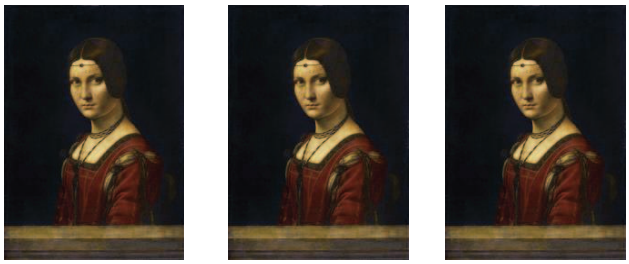


Fig.5. Labelle.bmp embedded with Renoir4-128.jpg (4.8 KB)

As can be seen in Figures 3 to 5, there are no visual differences between the cover image and the two stego images for each case, and between the three cases, despite the big difference in multimedia file sizes.

## V. CONCLUSION and FUTURE WORK

The experimental results that were obtained from embedding a collection of secret multimedia files within an uncompressed RGB BMP cover image have lead to the following conclusions:

1. It is possible to hide a large secret file within two uncompressed RGB covers, where the ratio of secret file to cover file sizes is <= 100%. To achieve the maximum hiding capacity embedding, the cover file size should be chosen to be near equal to the secret file size.

2. The PSNR value is inversely proportional to the secret-to-cover ratio (SCR), hence if imperceptibility has higher priority than hiding capacity, a larger cover file should be used.

3. Despite the full capacity hiding in the two covers, the resulting PSNR value was above 30 dB, which is acceptable regarding imperceptibility.

4. The secret file integrity was maintained, as the recovered files were identical to the original secret multimedia files in contents, size, and structure. There were zero differences between the original and recovered secret files.

The present work can be enhanced in future work to achieve stronger security of hidden multimedia files. The following suggestions are presented for possible areas of enhancement:

- Embedding multiple secret files in multiple cover images, using the concept of vertical splitting of a secret file.
- Extending the dual cover concept into other media such as audio and video.
- Strengthening the security of the proposed model through random placement of the secret data between the two covers.

ACKNOWLEDGMENT

The authors acknowledge the use of the publically available multimedia files and images, citations to their sources are stated in the dataset website [11].

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran, & P. McKevitt, "Digital image steganography: survey and analysis of current methods", Signal Processing, 90(3), 727-752, 2010.
[2] R. R. Koppola, "A high capacity data-hiding scheme in LSB-based image steganography, Master thesis, University of Akron, 2009.
[3] T. Morkel, "Image steganography applications for secure communication, Master thesis, University of Pretoria, 2012.
[4] G.R. Manjula & Ajit Danti, "A novel hash based least significant bit (2-3-3) image steganography in spatial domain", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, 2015.
[5] M. Qasem, "Hiding secret image within RGB images using an enhanced LSB method", Master thesis, Middle East University, Amman, Jordan, 2014.
[6] A. D. Ker, "Batch steganography and the threshold Game", in Security, Steganography, and Watermarking of Multimedia Contents IX, volume 6505 of Proc. SPIE, pages 04 1–13, 2007.
[7] H. G. Schaathun, "Machine learning in image steganalysis", John Wiley & Sons, 2012.
[8] A. Aljarf, S. Amin, J. Filippas, & J. Shuttelworth, "Develop a detection system for grey and colour stego images", International Journal of Modeling and Optimization, 3(5), 2013.
[9] A. Aljarf & S. Amin, "Filtering and Reconstruction System for Grey-Level Forensic Images", 17th International Conference on Image Processing (ICIP 2015) Zurich, Switzerland, 2015.
[10] K. Joshi, K., & R. Yadav, "A new LSB-S image steganography method blend with Cryptography for secret communication", 2015 Third International Conference on Image Information Processing (ICIIP), pp. 86-90, IEEE, 2015.
[11] M. T. Al-Bayati & M. M. Al-Jarrah, "DuoHide Steganography Dataset", available online on: www.duohide.com, viewed on 30/6/2016.
[12] M. T. Al-Bayati, "The hiding of multimedia secret files in dual RGB cover images using LSB steganography techniques, Master thesis, Middle East University, Amman, Jordan, 2016.