

Enhance the Hiding Image by Using Compression and Securing Techniques

Ahmed S. Farhan¹, Fouad H. Awad², Saif Saad³

¹College of Business Informatics /University of Information Technology and Communications
ahmeedsuliman@gmail.com

² College of Business Informatics /University of Information Technology and Communications
fouad_h_89@uoitc.edu.iq

³ College of Computer science and Information Technology\ University of Anbar
dovewhite89@gmail.com

Abstract: Information security is a huge trending topic in recent year. Many technique and algorithm were designed and developed to achieve the security of information and/or network across the world. Cryptography is one of the most common tools to provide such security. Nevertheless, steganography also provide a good security by hiding data within a media in a way that an attacker can't sense the presence of the secret data. Compression don't normally imply any security, however, it messes up the original encoding of the data and reduces its size by a measureable amount which makes it perfect for hiding. In this paper a system was proposed where a secret image is compressed before encryption and hiding. JPEG algorithm was used for the compressing, while at the encryption stage RC4 algorithm was used due to its fast processing speed. LSB (Least Significant Bit) technique then applied to hide the secret data within the cover image.

Keywords: Encryption, RC4, Hiding, Cryptography, Steganography.

1- INTRODUCTION

Information and networks security are becoming highly important in recent years. The rise of demand for the security solutions comes from the rapid development of technology. Security attacks can significantly affect the data exchange of an organizations' network. There are several methods and solutions to these attacks. Some relates to secure the data itself while the others relay on securing the media on which the data is being transferred [1]. Here in this paper, a technique is introduced that combines compression, encryption and hiding to secure images.

2- COMPRESSION

Compressing an image can be expressed as reducing the number of bits that are needed to represent that image with the same or lower (accepted) quality. Image compression does not imply any cryptography although it transforms the image into another format. Instead, the compression process only insures that the size of the compressed image is lower by a significant amount [2].

3- CRYPTOGRAPHY

Cryptography refers to the science of encrypting/encoding a piece of plaintext and resulting in cipher text which is non-readable except to the entities that share the right to read it. The encryption process composes of several mathematical and/or other transformations that generate the cipher text. The cipher text is a coded form of the original data; it is not hidden or secret. The encryption process can be reverted back to retrieve the original plain text by Decryption. Many encryption standards exist to achieve security, authentication and integrity[3]. Examples of these standards are DES, AES, RC4, SHA1 and RSA and many others with different goals and methods.

4- STEGANOGRAPHY

Steganography is basically a method of hiding some info inside a file. It does not imply any encryption. Instead, the info will only be invisible. Steganography normally uses a cover media into which the secret data will be hidden. The cover media that carries the secret data is called stego medium. The process of steganography involves hiding the data in a way that it can't be sensed or detected and leaves no remarkable track about the original data.

Steganography are divided into 4 different [4]:

1. Text.
2. Image.
3. Audio.
4. Video.

1- Text Steganography: They have a very small amount of redundant data; therefore they are very often unused.

2. Audio/Video Steganography: Their complexity makes them rarely used.

3- Image Steganography: It's the most common used method of steganography due to its redundant data. Images provide the easiest and fastest way to hide and transfer the information over the internet. It includes many categories:

- a. Transform Domain: Includes JPEG.
- b. Spread Spectrum: Includes patch work.
- c. Image Domain: Includes (LSB and MSB) in BMP and JPG.

5- RELATED WORK

A technique of encryption and hiding was proposed by Hemlata, Mithlesh and Dinesh. The technique uses encryption on the secret image first and it's done by the BLOWFISH algorithm due to the good performance it has. After that the encrypted image is embedded into video using

LSB method for hiding. By applying encryption to secret image before hiding, their proposed system satisfies some basic key aspects of data security like: Authenticity, Confidentiality and Integrity [5].

Another technique was proposed by Rasha and Sawsan uses different combination of encryption and hiding. First the image is transformed from the time domain to frequency domain by using discrete wavelet decomposition technique (Haar). Then comes the text encryption which is done with two algorithms (RC4 and Rijndael). The last step is embedding the encrypted text to the image using Least Significant Bit (LSB) technique. Their method was test on various images and showed good results of hiding according to (PSNR) equation [6] [7].

Domenico and Luca proposed a method of combining cryptography and steganography together by using images as covers for steganography and as key for cryptography. Their system uses image processing to provide effective method from both stenographic and cryptographic perspective [8].

6- RC4 ALGORITHM

RC4 was developed by Ron Rivest in 1987. It is a variable-key-size stream cipher. The algorithm generates random sequence of bits to produce the key. RC4 runs very quickly and thus it's more preferable for such kind of encryption. The implementation of the RC4 algorithm is shown in the below figure (1).

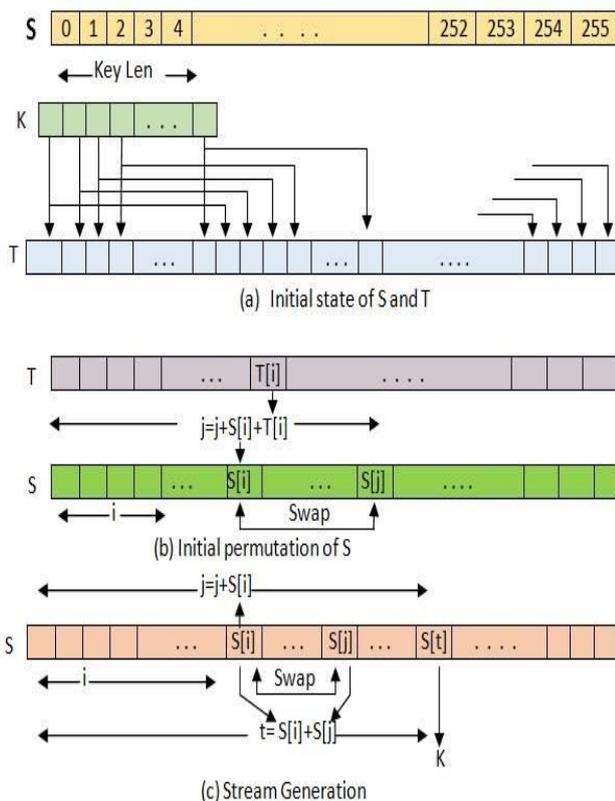


Figure 1: Steps of RC4.

7- THE PROPOSED SYSTEM

In this paper, a method is proposed for hiding secret image in another image. The secret image is first compressed by using JPEG algorithm to reduce its size. After compression the image enters the encryption phase which is done by RC4 algorithm to add more security before the hiding process. Then the secret image is embedded to the cover image by

using Least Significant Bit (LSB). The proposed method contains two phases, the embedding, as shown figure (2) and extraction, as shown in figure (3).

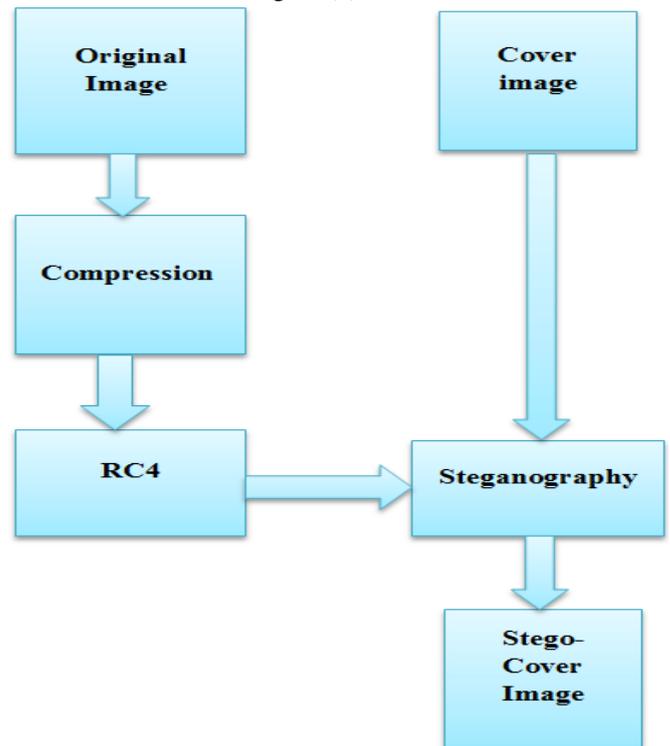


Figure 2: Steps embedding.

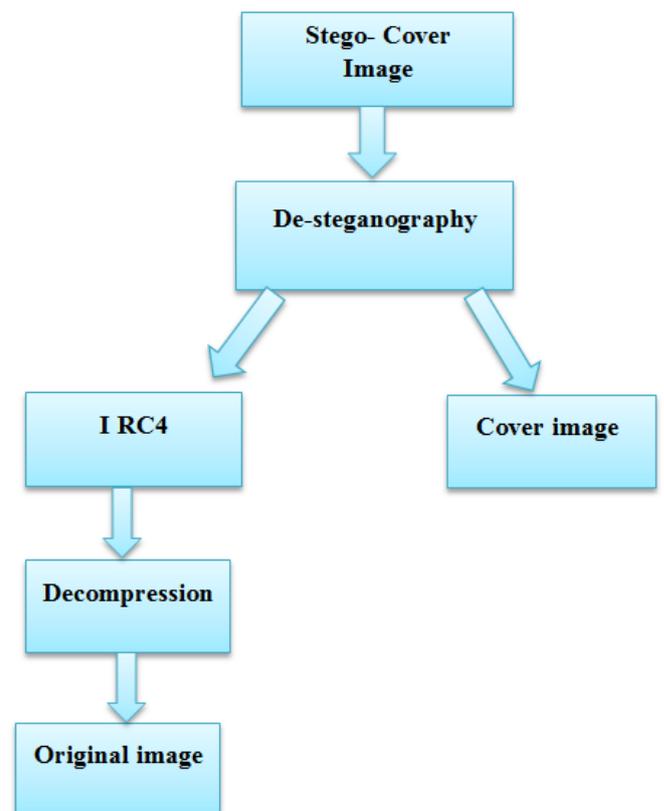


Figure 3: Steps of Extraction

- 1- Embedding Phase: The embedding phase contains:
 - A- Compression secret image (original image) by using JPEG algorithm to reduce size of image to half or more.
 - B- Encrypt original image will be hidden in cover image, the image encrypted by RC4 method.
 - C- Hiding secret image in the high frequency coefficient of cover image by using the LSB (Least Significant Bit) algorithm.
- 2- Extraction Phase: The Extraction Phase contains:
 - A- Extract the original image from cover image.
 - B- Decrypt the original image by decryption of RC4 algorithm.
 - C- Take the inverse compression image to return the image to original size.

8- IMPLEMENTATION AND RESULT

During the implementation phase, the used images are of type (JPEG) with different sizes. For the first image, the cover image was 1.16 MB while size of the original image was 48 KB and the Peak Signal to Noise Ratio (PSNR) was 65.93, Compression Ratio (CR) is (1:11.08). For this first image, the time of encryption was 0.0009 second and time of steganography was 0.0031second. The 5th image was of size 514 K while the size of original image (secret image) was 768 K and the Peak Signal to Noise Ratio (PSNR) was 52.15, CR is (1:10.06). The time of encryption was 0.0079 second and time of steganography was 0.0242 second. The last image was of size 768 K while the size of the original image was 769 K and the Peak Signal to Noise Ratio (PSNR) was (55.31), CR is (1:20.92).The time of encryption was 0.0038 second and time of steganography was 0.0124second, as shown in table 1.

Table 1: The Results

No.	Size of cover image	Size of original image (secret)	PSNR	CR	Time of encryption	Time of Steganography
1	1.16 M	48 k	65.93	1:11.08	0.0009 s	0.0031 s
2	1.16 M	192 k	61.83	1:16.11	0.0032 s	0.0052 s
3	1.16 M	769 K	57.42	1:20.92	0.0030 s	0.0109 s
4	514 K	1.16 M	55.38	1:36.15	0.0036 s	0.0104 s
5	514 K	768 K	52.15	1:10.06	0.0079 s	0.0242 s
6	514 K	15.1 K	59.06	1:14.23	0.0019 s	0.0049 s
7	192 K	48 K	58.49	1:11.08	0.0009 s	0.0018 s
8	15.1K	11.1 K	54.16	1:17.42	0.0012 s	0.0038 s
9	1.16 M	1.16 M	57.83	1:36.15	0.0013 s	0.0110 s

10	768 K	769 K	55.31	1:20.92	0.0038 s	0.124 s
----	-------	-------	-------	---------	----------	---------

9- CONCLUSION

In this paper, a technique is introduced for hiding secret image in another image using JPEG algorithm for compression, RC4 for encryption and LSB for hiding. JPEG algorithm is applied to reduce the size of secret images by measureable amount, while RC4 algorithm is used to highly secure the image data before embedding. The evaluation of the proposed method shows good performance and the stego-image cannot be distinguished from the original image. Also the proposed system operates efficiently and quickly in terms of memory and CPU.

REFERENCES

- [1] Satinsown,D.”Cryptography:Theory and practice”.
- [2] RatinderKaur,V.K.Banga “Image Security using Encryption based Algorithm” International Conference on Trends in Electrical,Electronics and Power Engineering(ICTEEP 2012)July 15-16,2012 Singapore.
- [3] Zaidoon kh.AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi “Overview: Main Fundamentals for Steganography” Journal of computing,Volume 2,Issue 3,March 2010 ISSN 2151-9617
- [4] Advanced Steganography Algorithm using encrypted secret message ,JoyshreeNath and AsokeNath, International Journal of Advanced Computer Science and Application(IJACSA) Vol-2 No.3,Page 19-24 ,March 2011.
- [5] Hemlata Sharma, MithleshArya, Dinesh Goyal “ Secure Image Hiding Algorithm using Cryptography and Steganography” IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 13, Issue 5 (Jul. - Aug. 2013), PP 01-06.
- [6] CHANDRESH K PARMAR, PROF.KRUTI PANCHOLI “A REVIEW ON IMAGE COMPRESSION TECHNIQUES” JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN ELECTRICAL ENGINEERING ISSN: 0975 – 6736| NOV 12 TO OCT 13 | VOLUME – 02, ISSUE – 02.
- [7] Rasha H.Ali , Sawsan H.Jaddoa “HIDING SECRET TEXT IN IMAGE USING RC4 AND RIJINDEAL ALGORITHM” INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY Volume 6, Issue 1, January (2015), pp. 12-18.
- [8] Domenico Bloisi and Luca Iocchi “IMAGE BASED STEGANOGRAPHY AND CRYPTOGRAPHY” .
- [9] Robshaw, M. Stream Ciphers. RSA Laboratories Technical Report TR-701,http://www.rsasecurity.com/rsalabs/index.html, July, 1995.
- [10] The RC4 Stream Encryption Algorithm, William Stallings, fifth edition, 2005.