Multiple-Layered Securities Using Steganography and Cryptography

Abubaker Wahaballa, Osman Wahballa, Fagen Li, Mohammed Ramadan & Zhiguang Qin

MULTIPLE-LAYERED SECURITIES USING STEGANOGRAPHY AND CRYPTOGRAPHY

Abubaker Wahaballa,*,** Osman Wahballa,*,*** Fagen Li,* Mohammed Ramadan,*,*** Zhiguang Qin*

Abstract

This paper presents multiple-layered securities by combining steganography with cryptography under the scope of information hiding, and both image and audio steganography are used to obtain a more robust security system. Firstly, the different approaches of steganography and cryptography are discussed, and comparisons drawn between them. Secondly, the design of the dual-layered security system is presented. The algorithms for this work are based on the Least Significant Bit steganography and AES cryptography. The code has been implemented in C# and visual studio 2010 due to its object encryption/decryption abilities. Under the provisions of the system, if an attacker detects that steganography is being used, the embedded message cannot be read due to file encryption. Finally, Matlab analysis of the original and stego media quality effects are presented, proving the robustness of this type of security implementation.

Key Words

Steganography, cryptography, least significant bit

1. Introduction

Steganography [1] is the science or art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means covered writing. It includes a vast array of secret communications methods that conceal the messages very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications.

Cryptography [2] is the science of writing in secret code and is an ancient art. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. Steganography and cryptography are relatives in information security field. Cryptography scrambles a message so it cannot be understood. Steganography hides the message into digital media [3].

* University of Electronic Science and Technology of China, Chengdu, China; e-mail: {fagenli, qinzg}@uestc.edu.cn
** National Council of Technical and Technological Education, Khartoum, Sudan; e-mail: wahaballah@hotmail.com
*** Karary University, Khartoum, Sudan; e-mail: wahballa 777@hotmail.com, nopatia@gmail.com
Recommended by Prof. H. Xu

By reference to dictionary.com [4]: steganography is "hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message" and cryptography is "the process or skill of communicating in, or deciphering the secret writing or ciphers." Steganography can be used to cloak hidden messages in cover media such as image, audio, video, protocol, or even text files. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, authentication, and data origin authentication. Cryptography is used in many cases such as e-mail communication, phone, fax, bank transaction, bank account security, credit card transaction, PINs, and spay-craft.

There are different types [5], [6] of steganography and cryptography to protect data and communication between sender and receiver, and prevents an attacker from trespassing the sensitive information. The types of steganography as shown in Fig. 1 can be divided into: plain text, image, audio, video, and TCP/IP steganography. On other hand, cryptography systems can be classified [7], [8] into two types: symmetric-key systems and asymmetric-key systems.

The data encryption standard (DES) was once a dominant symmetric-key algorithm for the encryption/decryption of data. It was developed at IBM in 1970 and based on an earlier design by Horst Feistel. This algorithm was approved and adopted by the National Bureau of Standards (now NIST) after the assessment of DES strength and modifications by the National Security Agency (NSA), and became a Federal standard in 1977. In 2000, NIST selected a new algorithm (Rijndael) to be the advanced encryption standard (AES). This will eventually replace DES.

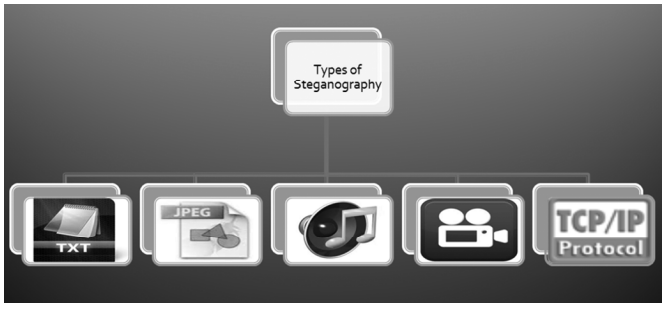

Figure 1. Types of steganography.

Table 1
Steganography versus Cryptography

Steganography	Cryptography
Steganography prevents discovery of very existence of communication	Encryption prevents an unauthorized party from discovering the contents of a communication
Little known technology	Common technology
Technology still being developed for certain formats	Most of algorithm known by all
Once detected message is known	Strong current algorithm are currently resistant to attack, larger expensive computing power is required for cracking
Steganography does not alter the structure of the secret message	Cryptography alter the structure of the secret message

RSA is the most widely deployed public-key (asymmetric key) cryptosystems and is used to transmit data securely over insecure and public channel. This type uses a pair of keys; one for encryption which is public and another for decryption which is kept secret. RSA was developed by three professors at MIT in 1977, Ron Rivest, Adi Shamir, and Leonard Adleman, their initials give the algorithm its name. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

Steganography must not be confused with cryptography, where we transform the message so as to make its meaning obscure to malicious people who intercept it. Therefore, the definition of breaking the system is different. Joseph and Sundaram [9] summarized this difference in Table 1.

Stallings [10] describes computer security as a: "... battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them". The motivation of this work is providing a secret and secured communication between people by design dual-layered security measures utilizing the following techniques:

- *Steganography*: to hide and unhide (stego and destego) text message in digital media (image or audio);
- *Cryptography*: to encrypt and decrypt the text message.

When we combine steganography and cryptography techniques together, we can get powerful method which enables people to communicate in secret way without possible eavesdroppers even knowing there is a form of communication in the first place.

2. Related Works

Previous researches [3], [11]–[14] suggested the combination of steganography and cryptography. However, up to now only one of these techniques was implemented at any one time (steganography or cryptography). From previous research, many weaknesses are apparent. In 2005, Jithesh and Kumar [15] proposed combining both steganography and cryptography for multiple layer information masking, two algorithms were proposed; the first being a discrete cosine transform coupled with a new cryptographic technique, namely visual cryptography; this idea was put forth but never implemented. In 2006, Dang and Kota [16] implemented a secure system with both steganography and cryptography. The encryption and decryption algorithms are implemented using C.Net libraries in the DES and RSA algorithms. The advantages of this type of implementation are the provision of three levels of security; compression, encryption, and steganography. The disadvantages are that the effects of stego media are not represented, and detailed design algorithms are not provided, such as pseudo code and flow charting. Recently in 2011, Kumar *et al.* [17] enhanced this technique to improve robustness in steganography, a multiple watermark embedding algorithm was proposed to embed multiple text messages as watermarks simultaneously in a single image. The advantage of this is a designed robust watermark which can be decoded or detected without affecting the original image quality. Thus, this method is robust at high levels to unintentional attacks such as JPEG compression or transcoding. However, the proposed method focuses on watermark steganography rather than a combination with cryptography. In the past year Madhavarao *et al.* [18] suggested a combination of steganography with cryptography. There are many implied weaknesses in this proposition, these weaknesses are surmized in a single point; a short survey about steganography and cryptography was presented, however a suitable scheme was not presented, nor was an algorithm or method to create this combination stated. In April of the same year Vivek *et al.* [19] proposed a powerful technique to implement steganography and cryptography together. This technique was described as follows:

1. Find the shared stego-key between the two communication parties by applying the DiffieHellman Key exchange protocol.
2. Encrypt the data using secret stego-key.
3. Select the pixels by an encryption process with the help of the same secret stage-key to hide the data.

This work was merely a proposed framework and was never implemented for analysis or testing. Currently the work in this paper seeks to correct the aforementioned vulnerabilities by combining steganography and cryptography concurrently to manipulate one data type.

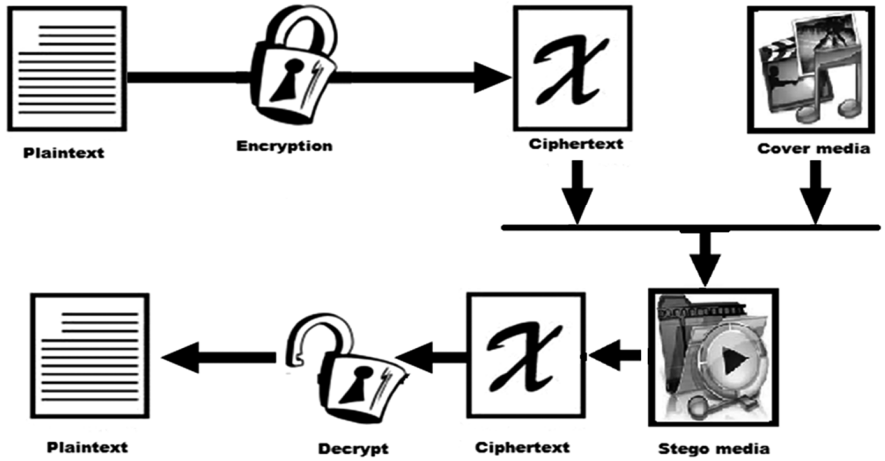

Figure 2. System structure.

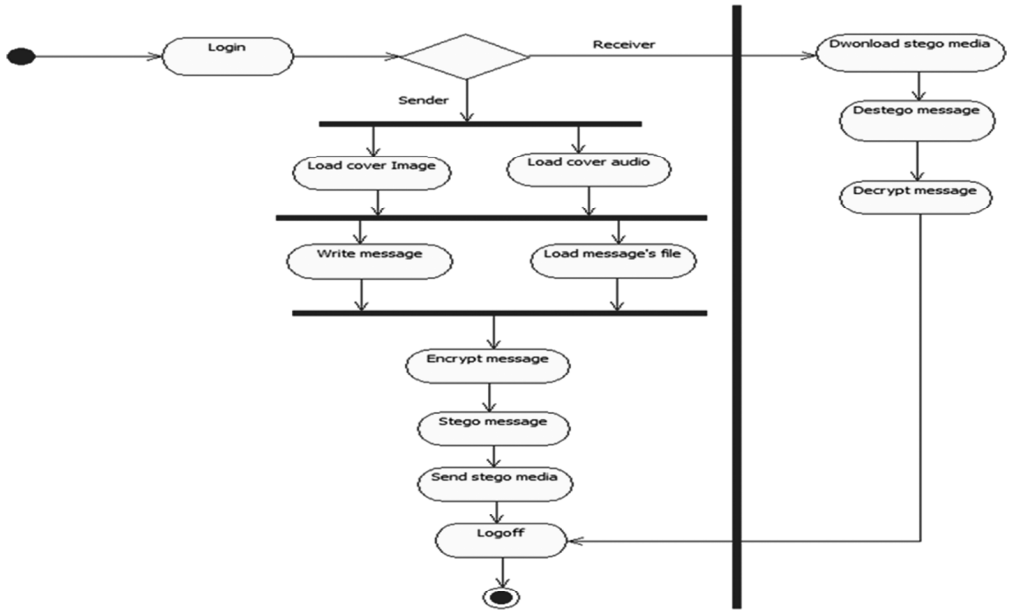

Figure 3. Activity diagram.

3. Model, Analysis, Design, and Implementation

The proposed model is expressed diagrammatically in Fig. 2. It allows the sender to encrypt a message, then hide or stego it in cover media. Also, it provides the receiver the ability to unhide or destego the message then decrypt it. The model also provides for the sending of stego media *via* e-mail using an e-mail sender. This model aims to achieve high levels of simple and flexible security.

3.1 Analysis and Design with UML Notations

The unified modeling language [20] is a language for specifying, constructing, visualizing, and documenting the software system and its components. It was created by Object Management Group (OMG) and UML 1.0. The UML uses mostly graphical notations to express the design of software projects. UML offers a way to visualize a system's architecture in diagrams. These diagrams are categorized into:

- Structural diagrams which include class diagram, object diagram, component diagram, and deployment diagram.
- Behavioral diagrams which include use case diagram, sequence diagram, collaboration diagram, state chart diagram, and activity diagram.

In this paper, we use the activity diagram to represent the sender's and receiver's behaviors in Figure 3. First, the sender logins to the system, then he loads the cover media (image or audio), writes or loads a message, encrypts a message, stego message in cover media, and sends the stego media through e-mail as an attached file. Then, the receiver downloads stego media from the e-mail, then extracts and decrypts a message. The solid black circle on the left shows the beginning of activities, and the white circles with black dots in the center denote where activities end.

3.2 Steganography and Cryptography Algorithms

The designed algorithms for this work are Least Significant Bit (LSB) to Steganography and AES to Cryptography. The LSB is the lowest bit in a series of numbers in binary. LSB algorithm replaces the least significant bits of each pixel (byte) in image by the hidden message bits.

Algorithm 1: LSB embedding

Input: $coveMedia, Msg$
Output: $stegoImg$

$Bit \leftarrow M_0, M_1, .., M_{65535}$ // Extract Bit set of Msg
$Pixel \leftarrow pixel_0, pixel_1, .., pixel_{65535}$ // The pixels of cover media
$LSB \leftarrow A_0, A_1, .., A_{65535}$ // Extract LSB set of the cover media
$SineS \leftarrow B_0, B_1, .., B_{65535}$// Extract SentinelString set of the cover media
for $i \leftarrow 1$ ***to*** $Msg.length$ **do**
  if $M_i = B_i$ **then**
    $donothing$
    else if $M_i = 1$ **and** $B_i = 0$ **then**
      $B_i \leftarrow M_i$
      $A_i \leftarrow 0$
      $Pixel_i \leftarrow Pixel_i - 1$
    else if $M_i = 0$ **and** $B_i = 1$ **then**
      $B_i \leftarrow M_i$
      $A_i \leftarrow 1$
      $Pixel_i \leftarrow Pixel_i + 1$
return $stegoImg$

Algorithm 2: LSB extract

Input: $stegoImg$
Output: $Plaintext$

$OutterSearch \leftarrow 1$
$InnerSearch \leftarrow 1$
$StopSearch \leftarrow 1$
$count \leftarrow 0$
$leftCounter \leftarrow 0$
$rightCounter \leftarrow 0$
while *(count* $<$ *(StegoImg* $-$ *SineS.Length)* **and** *StopSearch* $= 0$*)* **do**
  if $StegoMedia[count] = SienS[0]$ **then**
    $leftCounter \leftarrow count + 1$
    $rightCounter \leftarrow 1$
    $InnerSearch \leftarrow 1$
    while *(InnerSearch* $= 1$*)* **and** *(rightCounter* $<$ *SineS.Length)* **and** *(leftCounter* $<$ *StegMedia.Length)* **do**
      if *(rightCounter = (SineS.Length* $- 1$*))* **then**
        $StopSearch \leftarrow 1$
        else
          $InnerSearch \leftarrow 0$
          $count \leftarrow count + 1$
    else
      $count \leftarrow count + 1$
if $StopSearch = 1$ **then**
  while *(leftCounter* $<$ *StegImg)* **do**
    $Plaintext \leftarrow StegoImg[leftCounter]$
    $leftCounter \leftarrow leftCounter + 1$
else
  $ThePictureDoesNotContainAnyText$
return $Plaintext$

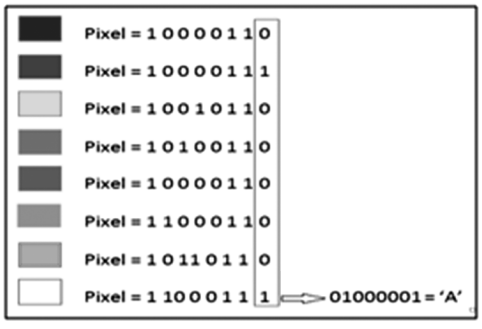

Figure 4. Replaced in LSB algorithm.

Figure 4 shows that. In our software we used Bmp 256 colours as a cover image and JPG, JEPG, or GIF as embedded images. So, we can hide a message up to 65,536 bytes. The message is embedded in the Sent-in-element-String (SineS) of the cover to increase the robustness of the system and protect the message against the external influences such as noise, filter, compression, *etc*. The embedding algorithm replaces the permutated bits of the message (M) by the SineS set of the cover image to obtain the new stego image. Algorithm 1 shows the pseudocode to embed the message in cover media, while Algorithm 2 shows the instruction to extract the message from the stego media.

Algorithm 3: AES

Input: *Plaintext*
Output: *ciphertext*

Parameters:
$Nb \leftarrow 4$ // block size (in words): no of columns in state (fixed at 4 for AES)
$Nk \leftarrow key.length/4$ // key length (in words): 4/6/8 for 128/192/256-bit keys
$Nr \leftarrow Nk + 6$ // no of rounds: 10/12/14 for 128/192/256-bit keys
$KeyExpansion(bytekey[4 * Nk], wordw[Nb * (Nr + 1)], Nk)$ // The KeyExpansion routine
$i \leftarrow 0$
$w \leftarrow [(Nb * (Nr + 1)]$
$tmp \leftarrow [4]$
while $(i < Nk)$ **do**
  $w[i] \leftarrow word(key[4 * i], key[4 * i + 1], key[4 * i + 2], key[4 * i + 3])$
  $i \leftarrow i + 1$
$i \leftarrow Nk$
while $(i < Nb\ ^* (Nr + 1))$ **do**
  $tmp \leftarrow w[i - 1]$
  if $(imodNk = 0)$ **then**
    $tmp \leftarrow SubWord(RotWord(tmp))xorRCON[i/Nk]$
  else if $(Nk > 6)$**and**$(imodNk = 4)$ **then**
    $tmp = SubWord(tmp)$
  $w[i] = w[i - Nk]$**xor**tmp
  $i \leftarrow i + 1$
return *ciphertext*

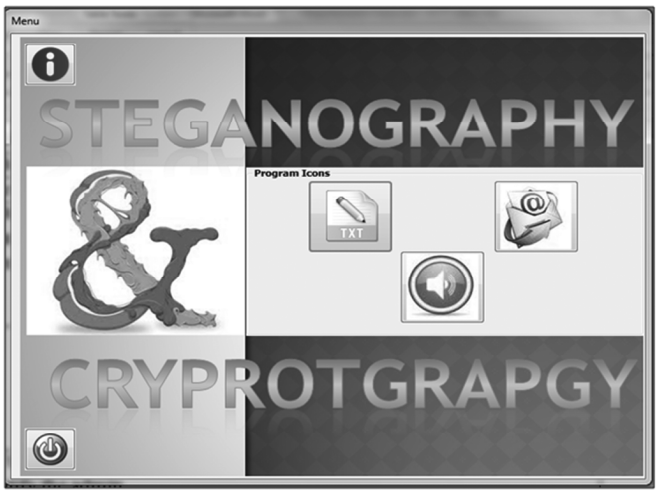

Figure 5. Menu screen.

User can select from this options:
– Click on txt icon to image steganography.
– Click on audio icon to audio steganography.
– Click on the e-mail icon to send e-mail.
– Click on about an icon to get help.
– Click on turnoff icon to turn off the system.

The AES, or Rijndael algorithm [21], is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Symmetric key algorithms are algorithms that use the same key to encrypt and decrypt data. The AES algorithm allows using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. AES has been selected and adopted by the US National Institute of Standards and Technology (NIST)

Figure 6. Image steganography screen.

Image steganography options:
– User (sender) loads cover image first.
– Writes the plain text.
– Clicks button encrypt to encrypt the plain text.
– Selects stego option, then clicks button stego/destego.
– The system will send the message stego successfully.

If Receiver
– Load stego image first.
– Select destego option, then click button stego/destego.
– The cipher-text will appear in the bottom text area, then click button decrypt.

as a new standard symmetric key encryption algorithm, from 15 qualifying algorithms and is now used world-wide. NIST has also made efforts to update and extend their

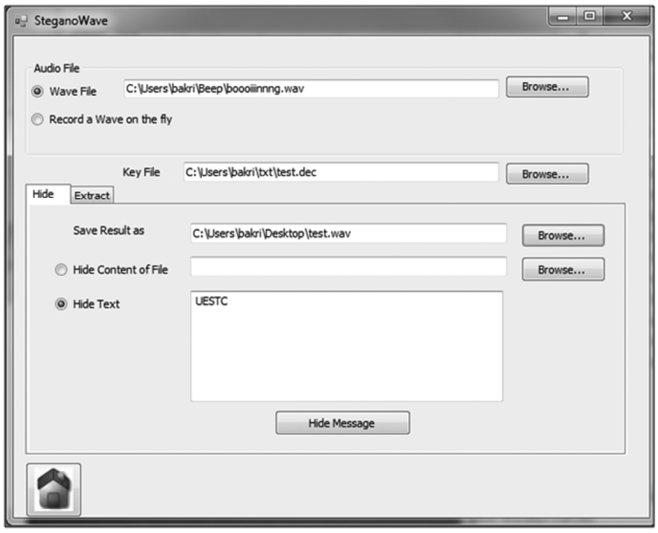

Figure 7. Audio steganography screen.

Audio steganography options:
– User (sender) selects record wave or load wave file.
– User loads the key file.
– User writes text or loads txt file.
– User saves the wav file.
– User clicks button hide message.

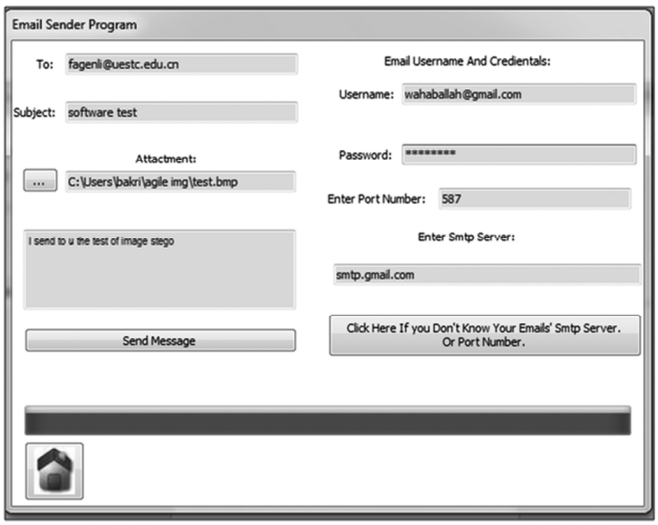

Figure 8. E-mail sender screen.

Email sender instructions:
– Sender adds receiver e-mail address.
– Sender attaches the stego media.
– Then clicks send message button after filling the information on the right.

standard cryptographic modes of operation. In this work, we use AES encryption designed by C# as an encapsulated component to encrypt and decrypt the text. The AES pseudocode is shown in Algorithm 3.

Table 2
Analysis Result of Original and Stego Media

Same Media Size 312 KB and Same Text	MSE	RMSE	PSNR
Images	0	0	INF
Waves	$3.3029e^{-008}$	$1.8174e^{-004}$	122.9758

3.3 Graphic User Interface (GUI)

The software of this work is developed with Graphic User Interface (GUI), which is simple and easy to use, which allows users to login first and then select which type of steganography is required (image or audio) as shown in the main screen in Fig. 5. Figures 6 and 7 display the image and audio steganography and cryptography, the last of GUI. Figure 8 displays the e-mail sender screen which allows users to send the stego media over Internet through e-mail.

4. Analysis Media using Matlab

Two types of media data are used, these are image and audio. To measure the quality effect of this media three parameters were analysed [22]. These are Mean Squared Error (MSE), Root Mean Square Error (RMSE), and Peak Signal-to-Noise Ratio (PSNR) for original, and stego media and the differences noted. Table 2 shows a comparison between the two media used in the system, a wave and image to hide the same message. We found that the image file has not been affected, while the message size may have influenced the wave file. Also, they are represented graphically in Fig. 9.

1. MSE: It is the average squared difference between an original and stego media, as shown in formula (1). It is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count. For media $A = \{a_1..a_M\}$ and $B = \{b_1..b_M\}$, where M is the number of pixels:

$$MES(A,B) = 1/M \sum_{i}^{m} (a_i - b_i)^2 \qquad (1)$$

2. $PSNR$: It is the ratio between the original signal and the stego signal in a media, given in decibels. The higher the PSNR, the closer the stego media is to the original. In general, a higher PSNR value should correlate to a higher quality media, but tests have shown that this is not always the case. However, PSNR is a popular quality metric because it is easy and fast to calculate while still giving okay results (formula (2)). For media $A = \{a_1..a_M\}$, $B = \{b_1..b_M\}$, and MAX equal to the maximum possible pixel value ($2^8 - 1 = 255$ for 8-bit media):

$$PSNR = 10 \log 10 \left(\frac{MAX^2}{MSE(A,B)} \right) \qquad (2)$$

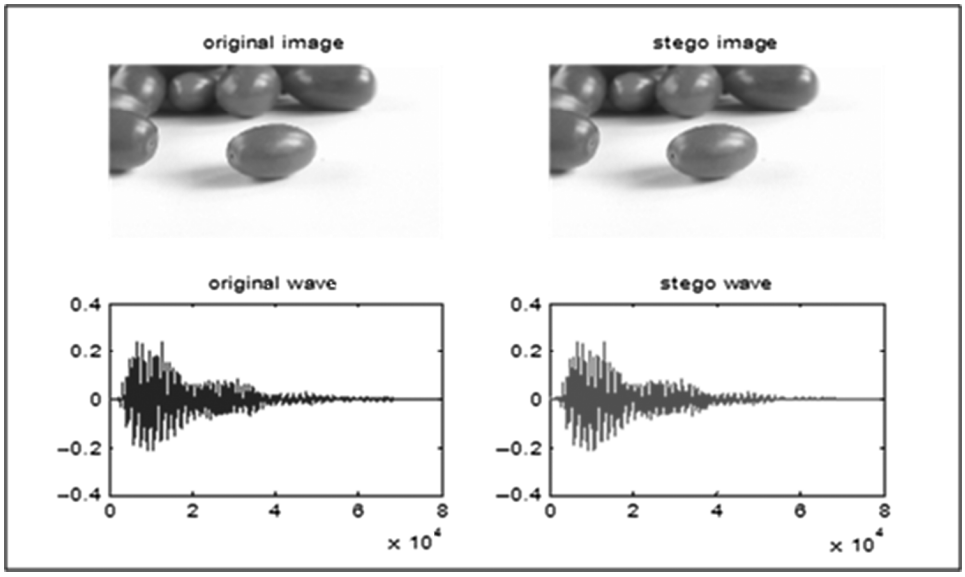

Figure 9. Original and stego media analysis.

3. $RMSE$: It is a measure of the differences between values predicted by a model or an estimator and the values actually observed from the thing being modelled or estimated. We can calculate RMSE in formula (3):

$$RMSE = \sqrt{(MSEE(A, B))} \tag{3}$$

Future works will focus on re-implementation of software to include other types of steganography such as video and TCP/IP protocol combined with other types of cryptography. Also, further options to send stego media instantly could be implemented, for example, in real-time chatting applications.

5. Conclusion

In this paper the developed software provides two layers of security cryptography and steganography in two forms, that are image and audio. Also, the software provides for the sending of stego media over the Internet *via* e-mail utilizing the SMTP protocol. This software improves security, reliability, and efficiency. The designed algorithms for this work are LSB steganography and AES cryptography. Under the provisions of the system, if an attacker detects the use of steganography, the embedded message is indecipherable due to message encryption, and *vice versa*.

Matlab analysis of the original and stego media quality effects are presented in this work. Also, evidence proving the robustness of this type of security is detailed.

Acknowledgement

This work is supported by the National Natural Science Foundation of China (Grant Nos. 61073176, 61272525, and 61272404) and the Fundamental Research Funds for the Central Universities (Grant No. ZYGX2013J069).

References

[1] N.F. Johnson and S. Jajodia, *Exploring steganography: Seeing the unseen* (IEEE Computer Society, 1998), ISSN: 0018-91628.

[2] R.S. Rajan and S. Tamilenthi, An overview of new trends in cryptography, *Recent Research in Science and Technology*, *4*(6), 2012, 38–42.

[3] D. Bloisi and L. Iocchi, Image based steganography and cryptography, *Proc. International Conf. on Computer Vision Theory and Applications (VISAPP)*, Barcelona, Spain, 2007, 8–11.

[4] http://dictionary.com

[5] B. Dunbar, *A detailed look at steganographic techniques and their use in an open-systems environment* (Information Security Reading Room, Washington, DC: Sans Institute, 2002).

[6] T. Morkel, H.E. Jan, and S.O. Martin , An overview of image steganography, *Proc. Fifth Annual Information Security South Africa Conf. (ISSA 2005)*, Sandton, South Africa, 2005.

[7] S. Goyal, A survey on the applications of cryptography, *International Journal of Engineering and Technology*, *2*(3), 2012, 352–355.

[8] A.J. Menezes, P.C. Van-Oorschot, and S.A. Vanstone, *Handbook of applied cryptography* (Boca Raton, FL: CRC Press, 2010).

[9] R.A. Joseph and V. Sundaram, Cryptography and steganography – A survey, *International Journal*, *2*(3), 2010, 626–630.

[10] W. Stallings, *Cryptography and network security principle and practice*, 5th ed. (Beijing: Publishing House of Electronic Industry, 2011).

[11] D.K. Sarmah and B. Neha, Proposed system for data hiding using cryptography and steganography, *International Journal of Computer Applications*, *8*(9), 2010, 7–10.

[12] K. Challita and F. Hikmat, Combining steganography and cryptography: New directions, *International Journal of New Computer Architectures and their Applications*, *1*(1), 2011, 199–208.

[13] K. Bailey and K. Curran, An evaluation of image based steganography methods, *Multimedia Tools and Applications*, *30*(1), 2006, 55–88.

[14] P.H.-W. Wong, O.C. Au, and Y.M. Yeung, Novel blind multiple watermarking technique for images, *IEEE Transactions on Circuits and Systems for Video Technology*, *13*(8), 2003, 813–830.

[15] K. Jithesh and D.A.S. Kumar, Multilayer information hiding – A blend of steganography and visual cryptography, *Journal of Theoretical and Applied Information Technology*, *19*(1/2), 2005, 109–116.

[16] X.H. Dang and C.S. Kota, Case study: An implementation of a secure steganographic system, *Proc. International Conf. on Security and Management (SAM 2006)*, Las Vegas, NV, 2006.
[17] S.P. Kumar, K. Anusha, and R.V. Ramana, A novel approach to enhance robustness in steganography using multiple watermark embedding algorithm, *International Journal of Soft Computing and Engineering (IJSCE)*, 2001, ISSN: 2231-2307 (online).
[18] E. Madhavarao, C.J. Raju, P. Divya, and A.S.K. Ratnam, Data security using cryptography and stegnography, *International Journal of Advanced Research in Computer Engineering and Technology*, *1*(5), 2012, 319–325.
[19] J. Vivek, K. Lokesh, M.S. Madhur, S. Mohd, and R. Kshitiz, Public-key steganography based on modified LSB method, *Journal of Global Research in Computer Science*, *3*(4), 2012, 26–29.
[20] A. Bahrami, *Object oriented system development* (Singapore: The McGraw-Hill Companies, 1999).
[21] R. Hosseinkhani and H.H.S. Javadi, Using cipher key to generate dynamic S-box in AES cipher system, *International Journal of Computer Science and Security*, *6*(1), 2012, 19–28.
[22] Q. Huynh-Thu and M. Ghanbari, Scope of validity of PSNR in image/video quality assessment, *Electronics Letters*, *44*(13), 2008, 800–801.

Biographies

Abubaker Wahaballa received the B.S. degree in computer sci-ence from Omdurman Islamic University in 2003, Khartoum, Sudan, and the M.S. degree in computer science-software engi-neering track form Sudan Uni-versity of Science and Technol-ogy in 2009, Khartoum, Sudan. He is currently working toward the Ph.D. degree in computer science from University of Elec-
tronic Science and Technology of China. His current research interests include information security, cryptography, steganography, and software agile.

Osman Wahballa received the B.S. degree in electrical engineer-ing and computer engineering from Karary University, Depart-ment of Electrical Engineering in 2006, Khartoum, Sudan, and the M.S. degree in M.Sc. in Com-puter Engineering, Information Security form University of Elec-tronic Science and Technology of China in 2013, Chengdu, China. He is currently working toward
the Ph.D. degree in computer science from University of Electronic Science and Technology of China. His current research interests include information hiding, steganography, and cryptography.

Fagen Li received his B.S. de-gree from Luoyang Institute of Technology, Luoyang, China, in 2001, M.S. degree from Hebei University of Technology, Tian-jin, China in 2004, and Ph.D. degree in cryptography from Xi-dian University, Xi'an, China in 2007. From 2008 to 2009, he was a postdoctoral fellow in Future University-Hakodate, Hokkaido, Japan, which is supported by the
Japan Society for the Promotion of Science. He worked as a research fellow in the Institute of Mathematics for Industry, Kyushu University, Fukuoka, Japan, from 2010 to 2012. He is now an associate professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China. His recent research interests include cryptography and network security. He has published more than 70 papers in the international journals and conferences.

Mohammed Ramadan received the B.S. degree in communica-tion engineering from Karary University in 2007, Khartoum, Sudan, and the M.S. degree in M.Sc. in computer engineering, information security from Uni-versity of Electronic Science and Technology of China in 2013, Chengdu, China. He is currently working toward the Ph.D. degree in Information Security, Mobile
Communication Security from University of Electronic Science and Technology of China. His current research interests include mobile communication and GSM security.

Zhiguang Qin received his Ph.D. degree in 1996 and is a Professor in UESTC presently. His research interests include information se-curity and computer network. He has published more than 50 pa-pers in international journals and conferences.